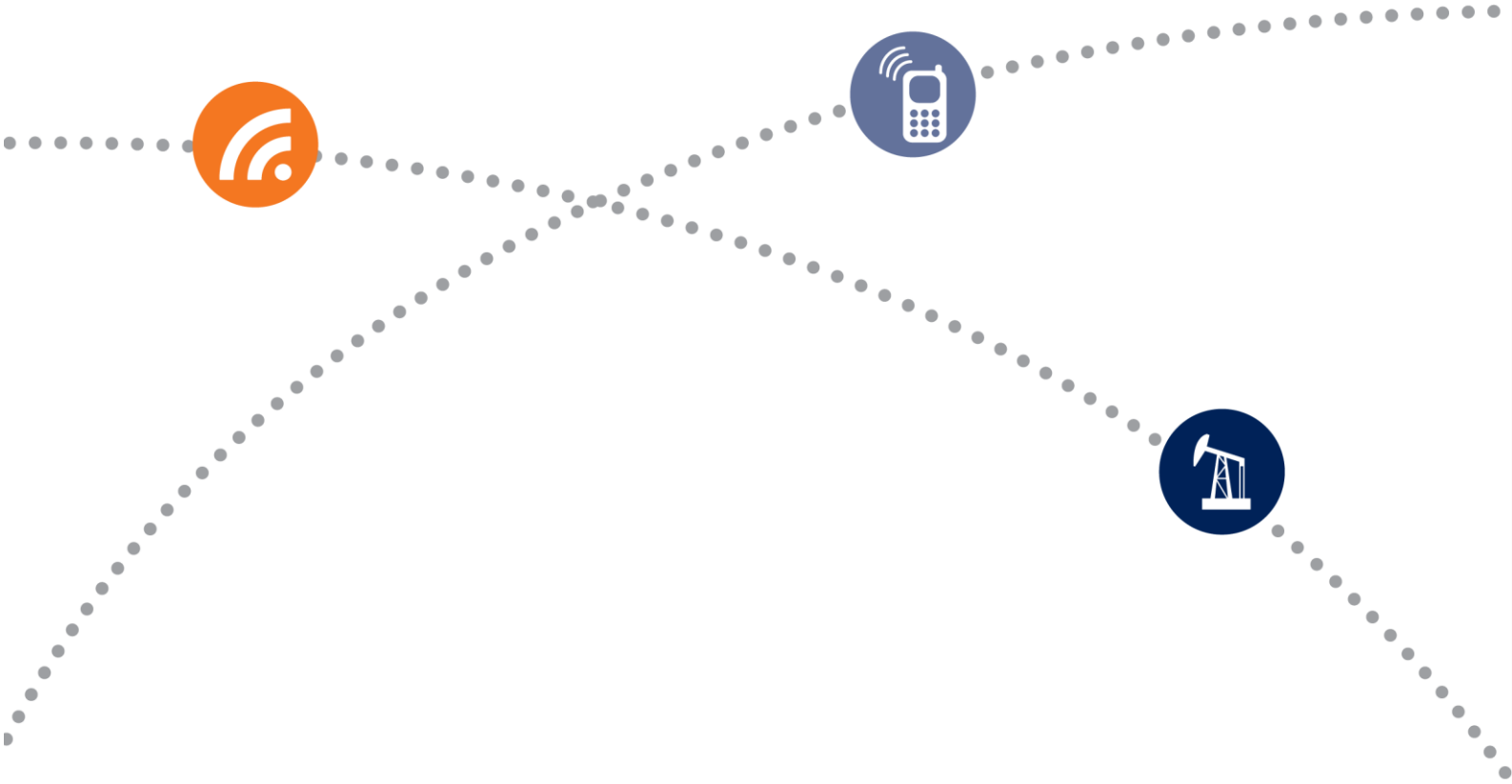

WBSIac Access Point

User Manual

Software Version:
January 2015
P/N

Legal Rights

© Copyright 2015 Alvarion Technologies Ltd. All rights reserved.

The material contained herein is proprietary, privileged, and confidential and owned by Alvarion or its third party licensors. No disclosure thereof shall be made to third parties without the express written permission of Alvarion Technologies Ltd.

Alvarion Technologies Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

Trade Names

Alvarion®, BreezeCOM®, WALKair®, WALKnet®, BreezeNET®, BreezeACCESS®, BreezeMAX®, BreezeLITE®, 4Motion®, and/or other products and/or services referenced herein are either registered trademarks, trademarks, trade names or service marks of Alvarion Technologies Ltd.

All other names are or may be the trademarks of their respective owners.

“WiMAX Forum” is a registered trademark of the WiMAX Forum. “WiMAX”, the WiMAX Forum logo, “WiMAX Forum Certified”, and the WiMAX Forum Certified logo are trademarks of the WiMAX Forum.

Statement of Conditions

The information contained in this manual is subject to change without notice. Alvarion Technologies Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

Warranties and Disclaimers

All Alvarion Technologies Ltd. ("Alvarion") products purchased from Alvarion or through any of Alvarion's authorized resellers are subject to the following warranty and product liability terms and conditions.

Exclusive Warranty

(a) Alvarion warrant that the Product hardware it supplies and the tangible media on which any software is installed, under normal use and conditions, will be free from significant defects in materials and workmanship for a period of fourteen (14) months from the date of shipment of a given Product to Purchaser (the "Warranty Period"). Alvarion will, at its sole option and as Purchaser's sole remedy, repair or replace any defective Product in accordance with Alvarion' standard R&R procedure.

(b) With respect to the Firmware, Alvarion warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from invoice date (the "Warranty Period")". During the Warranty Period, Alvarion may release to its Customers firmware updates, which include additional performance improvements and/or bug fixes, upon availability (the "Warranty"). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates.

Additional hardware, if required, to install or use Firmware updates must be purchased by the Customer. Alvarion will be obligated to support solely the two (2) most recent Software major releases.

ALVARION SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY PURCHASER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR IMPROPER TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

Disclaimer

(a) The Software is sold on an "AS IS" basis. Alvarion, its affiliates or its licensors MAKE NO WARRANTIES, WHATSOEVER, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. ALVARION SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT WITH RESPECT TO THE SOFTWARE. UNITS OF PRODUCT (INCLUDING ALL THE SOFTWARE) DELIVERED TO PURCHASER HEREUNDER ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE IN APPLICATIONS WHERE THE FAILURE, MALFUNCTION OR INACCURACY OF PRODUCTS CARRIES A RISK OF DEATH OR BODILY INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). HIGH RISK ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO, USE AS PART OF ON-LINE CONTROL SYSTEMS IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS OR OTHER APPLICATIONS REPRESENTING A SIMILAR DEGREE OF POTENTIAL HAZARD. ALVARION SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

(b) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT ALVARION'S OPTION. TO THE FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED. ALL OF WHICH ARE EXPRESSLY DISCLAIMED. ALVARION' WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. ALVARION NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Limitation of Liability

(a) ALVARION SHALL NOT BE LIABLE TO THE PURCHASER OR TO ANY THIRD PARTY, FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER ARISING UNDER BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE AND WHETHER BASED ON THIS AGREEMENT OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(b) TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE LIABILITY FOR DAMAGES HEREUNDER OF ALVARION OR ITS EMPLOYEES OR AGENTS EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT BY PURCHASER, NOR SHALL THE AGGREGATE LIABILITY FOR DAMAGES TO ALL PARTIES REGARDING ANY PRODUCT EXCEED THE PURCHASE PRICE PAID FOR THAT PRODUCT BY THAT PARTY (EXCEPT IN THE CASE OF A BREACH OF A PARTY'S CONFIDENTIALITY OBLIGATIONS).

Disposal of Electronic and Electrical Waste

Disposal of Electronic and Electrical Waste

Pursuant to the WEEE EU Directive electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Important Notice

This user manual is delivered subject to the following conditions and restrictions:

- This manual contains proprietary information belonging to Alvarion Technologies Ltd. Such information is supplied solely for the purpose of assisting properly authorized users of the respective Alvarion products.

- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of Alvarion Technologies Ltd.

- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.

- The software described in this document is furnished under a license. The software may be used or copied only in accordance with the terms of that license.

- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

- Alvarion Technologies Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

- The information contained herein is merely descriptive in nature, and does not constitute an offer for the sale of the product described herein.

- Any changes or modifications of equipment, including opening of the equipment not expressly approved by Alvarion Technologies Ltd. will void equipment warranty and any repair thereafter shall be charged for. It could also void the user's authority to operate the equipment.

About this Manual

This user manual is a guide to the WBSIac AP firmware on a wireless AP. WBSIac combines with the most advanced chipsets. WBSIac also includes a user-friendly web interface for the AP configuration.

This manual describes the WBSIac indoor access point and provides step-by-step instructions on how to get started, operate and manage the AP.

This manual contains the following chapters:

- Chapter 1 - "Overview"
- Chapter 2 - "Management"
- Chapter 3 - "Final Notes"
- "Glossary"

Contents

Chapter 1 - Overview 1

1.1 Introduction 2

1.2 Network Topology 2

1.3 Language 3

1.4 Supported Products 3

1.5 System Requirements 3

1.6 Getting Started 4

1.7 Operating Modes 5

1.8 Buttons and Changes 5

1.9 Physical Hardware Button 6

1.10 LEDs 6

Chapter 2 - Management 7

2.1 Status Tab 8

2.1.1 Overview 9

2.1.2 Routes 14

2.1.3 System Log 15

2.1.4 Realtime Graphs 15

2.2 System Tab 22

2.2.1 System 22

2.2.2 Administration 24

2.2.3 Services 27

2.2.4 SNMP 28

2.2.5 Physical Hardware Button 30

2.2.6 Backup / Flash Firmware 31

2.2.7 Reboot 32

2.3 Services Tab 33

2.3.1 Dynamic DNS 34

2.3.2 Hotspot 35
2.3.3 Discovery 42
2.4 Network Tab 43
2.4.1 Interfaces - WAN 44
2.4.2 Interfaces - AVLAN3316 48
2.4.3 Interfaces - LAN 49
2.4.4 Wifi - Overview 54
2.4.5 Wifi - Wireless Network 58
2.4.6 VLANs 69
2.4.7 Hostnames 71
2.4.8 Static Routes 72
2.4.9 Firewall 72
2.4.10 Diagnostics 79
2.4.11 Quality of Service 81
2.5 Arena Controller Tab 82
2.5.1 L2TPv3 Settings 82
2.5.2 IPSec 83
2.5.3 Arena Controller SNMP Settings 83
2.5.4 AP SNMP Settings 84
2.6 Logout 84
Chapter 3 - Final Notes 85
3.1 Troubleshooting 86
3.1.1 The PC Cannot Connect to the WBSlac AP 86
3.1.2 PC Ethernet and Wifi Adapters 86
3.1.3 The Mobile Phone Cannot Connect 87
3.1.4 The Mobile Phone Connects but cannot Access the Internet 87
3.1.5 Unresponsive Web Page 87
3.1.6 Unresponsive AP 88
3.2 Resetting to Factory Default 88
Glossary 89

Chapter 1 - Overview

In this Chapter:

- Introduction
- Network Topology
- Language
- Supported Products
- System Requirements
- Getting Started
- Operating Modes
- Buttons and Changes
- Physical Hardware Button
- LEDs

1.1 Introduction

WBSIac uses a free, clean, extensible and easily maintainable web user interface for embedded devices. It is high performance, has a small installation size, fast runtimes, and good maintainability.

The content of this guide is organized the same way as presented on the WBSIac AP's web page.

After the Login and Language sections, the following sections correspond to the top-level tabs:

- Status
- System
- Services
- Network
- Arena Controller

The last chapter contains the Final Notes which include troubleshooting information.

1.2 Network Topology

- A DHCP-enabled network (for the AP to obtain an IP address as well as for the wireless clients after deployment)
- For MESH network, MC or Cloud manager are running as Controller.

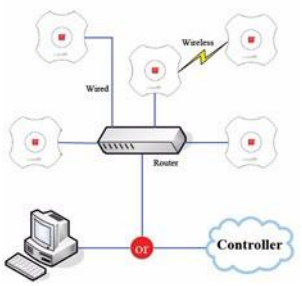

Figure 1-1: Network Topology

NOTE!

In the illustration in Figure 1-1, WBSIac is used as an example.

1.3 Language

To change the language, navigate to the **System** page, look for the **System Properties** section, click the **Language and Style** tab, and click the drop-down list for Language. You can change the language from English to another language e.g., Chinese.

1.4 Supported Products

The WBSIac software resides in the following models:

- WBSIac-2450-UN
- WBSIac-2450-EU
- WBSIac-2450-US

1.5 System Requirements

WBSIac supports the following operating systems:

- Microsoft Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Linux
- Mac OS X.

WBSIac supports the following web browsers:

- Mozilla Firefox
- Google Chrome
- Apple Safari
- Microsoft Internet Explorer 8 or above.

1.6 Getting Started

To access the WBSIac configuration interface, perform the following steps:

1 Connect the local area network (LAN) port of the WBSIac AP to the network port of your computer using an Ethernet cable.

Ethernet cables are also known as LAN cables or network cables. They connect devices such as computers, APs, and switches on wired networks.

2 Next, take the power adapter that comes with the set and connect it to a power socket as well as the WBSIac AP.

3 Assign the Ethernet adapter on your computer with a static IP address on the 192.168.1.x network, e.g., 192.168.1.10 and with a subnet mask 255.255.255.0.

4 Launch a web browser and enter the default IP address of the AP, 192.168.1.1, into the address bar.

The AP's configuration web page is displayed.

The first page that you see is the login page. The words on the top left denote the firmware build version, e.g., **WBSaci-1.01.00001**.

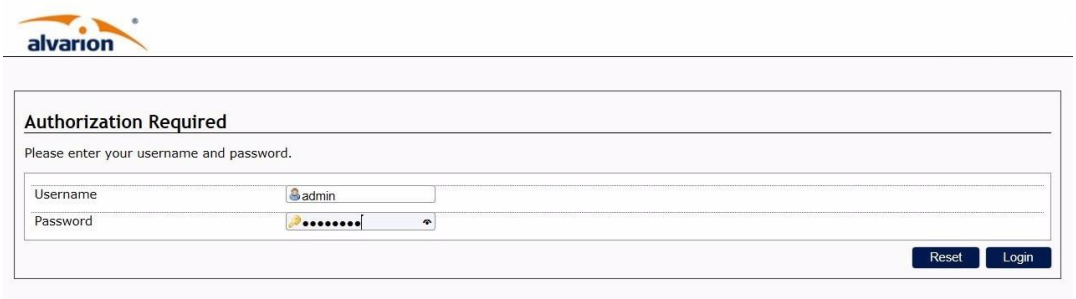

Figure 1-2: The WBSIac Login Page

The **Login Page** is presented when the WBSIac AP's IP Address is requested.

The default authorization details are:

- Username: **admin**
- Password: **password**

Advanced information: There is a 'root' user in the AP's Linux shell. It cannot be used to login to the AP's web page. Use the Arena Controller to change the password of the 'root' user to a password of your choice. Following that, you can access the AP's Linux shell by using a serial cable or by SSH. The PuTTY software can be used for either method. The Arena Controller software is offered free of charge.

1.7 Operating Modes

The WBSIac AP can operate in the following modes:

- Access Point / Master
- Station / Client
- Access Point WDS
- Station WDS

A wide area network (WAN) is a network that covers a broad area. The world's most popular WAN is the Internet.

In a commonly used setup, the WAN port of an access point connects to a modem via an Ethernet cable. A modem can be a cable, digital subscriber line (DSL), or fiber optic modem. A modem translates the signal from the internet service provider (ISP) to Ethernet signals that the access point can understand. This allows the access point to have internet connection.

Other devices called stations connect wirelessly to this access point. These devices can be mobile phones, printers, IP cameras, laptops, or even other APs. The stations obtain internet connection from the access point.

An access point WDS and a station WDS together extend the wireless coverage, like a repeater.

1.8 Buttons and Changes

The WBSIac buttons are described here.

- **Reset**: Click to undo any change(s).
- **Save**: Saves any change(s). Do not use this button currently.
- **Save & Apply**: Saves and applies any change(s). Use this button instead of the **Save** button for the change(s) to apply immediately. It is recommended to click this button before moving to a different page.
- **Logout**: Click to log out of the WBSIac AP's web page.

NOTE!

At the top right corner of the WBSIac AP's configuration web page, there may be one of the following texts displayed.

- **Changes: 0**: Means that all changes on the configuration web page have been applied to the WBSIac AP.
- **Unsaved Changes**: Shows the number of changes that were not saved and applied

1.9 Physical Hardware Button

For more information, refer to Section 2.2.5 Physical Hardware Button.

1.10 LEDs

LEDs are the light emitting diodes on the board.

After completing the connection, check the status of the LEDs.

Indicator	Name	Normal Status
	Power LED	Continuously on
	WAN LED	Continuously on
	LAN LED	Continuously on/Flashing
	Signal Strength	Increase from left to right

Chapter 2 - Management

In this Chapter:

- Status Tab
- System Tab
- Services Tab
- Network Tab
- Arena controller Tab
- Logout

2.1 Status Tab

After login, when you click on the Status top-level tab, the second-level tabs are displayed:

- Overview
- Routes
- System Log
- Realtime Graphs
- Hotspot Users

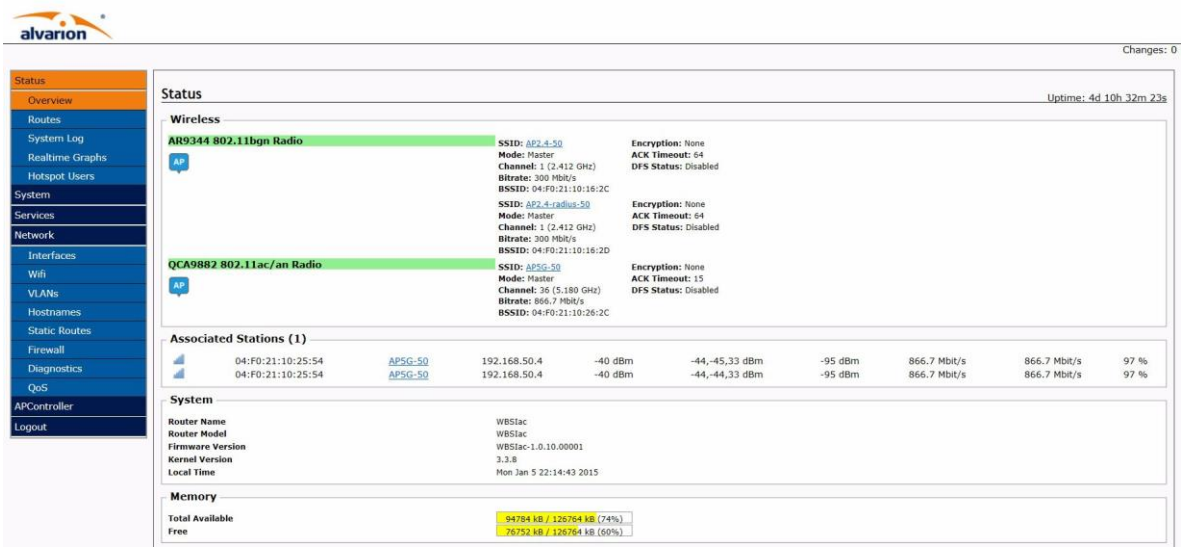

Figure 2-1: Status Page

Notice in the figure that the radio is using the latest and fastest 802.11ac wireless standard that supports a data rate of up to 866.7 Mbit/s.

2.1.1 Overview

The **Status** > **Overview** page is divided into the following sections:

- Wireless
- Associated Stations
- System
- Memory
- Network
- DHCP Leases

Uptime displays the duration of time since the WBSIac AP was turned on or rebooted.

2.1.1.1 Wireless

Figure 2-2: Wireless Chipset Model

The **Wireless** section in the **Status** > **Overview** page shows a summary of the wireless parameters. The following describes the parameters.

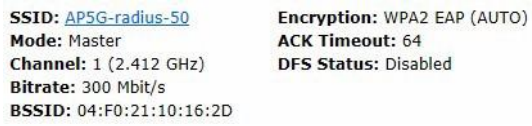

Figure 2-3: Wireless Parameters

The **Wireless** section shows a summary of the device operating as an 802.11ac access point.

- **SSID**: Displays the name of the wireless network that the access point (AP) is offering, the Service Set Identifier (SSID).
- **Mode**: This is 'Master' when the device is in AP mode or AP WDS mode.

- **Channel**: Shows the channel number and frequency that the AP is using.
- **Bitrate**: This is the maximum bitrate supported by the radio in the current configuration.
- **BSSID**: This is the MAC address of the AP's radio.
- **Encryption**: Displays the wireless encryption used.
- **ACK Timeout**: Shows the maximum acknowledgment time in microseconds.
- **DFS Status**: If DFS is enabled, the AP automatically switches channel if radar is detected on the current channel.

2.1.1.2 Wireless (for Station Mode)

The following describes the parameters for a device operating in Station mode.

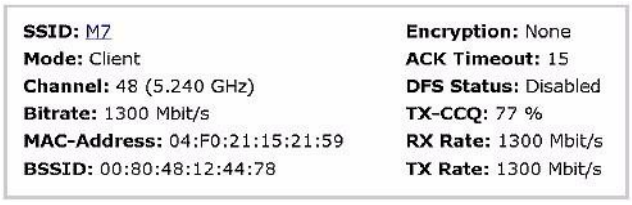

Figure 2-4: Wireless Parameters for Station Mode

The **Wireless** section shows a summary of the device operating as an 802.11ac station.

- **SSID**: Displays the name of the wireless network that the station should be associated with.
- **Mode**: This is 'Client' when the device is in Station mode or in Station WDS mode.
- **Channel**: Shows the channel number and frequency that this station is using. Normally, it would automatically select the same channel as the AP.
- **Bitrate**: This is the maximum bitrate supported by the radio in the current configuration.
- **MAC-Address**: States the MAC address of the device's radio.
- **BSSID**: This is the MAC address of the AP's radio.
- **Encryption**: Displays the wireless encryption used.
- **ACK Timeout**: Shows the maximum acknowledgment time in microseconds.
- **DFS Status**: If DFS is enabled, the AP automatically switches channel when radar is detected on the current channel.
- **TX-CCQ**: Displays the transmission quality in %. A higher percentage means a better wireless connection quality.
- **RX Rate:** Shows the receive bit rate of this station.
- **TX Rate**: Shows the transmit bit rate of this station.

2.1.1.3 Associated Stations (for AP Mode)

This section shows the connected devices, if the WBSlac AP is in the AP mode.

Figure 2-5: List of Associated Stations

If there are no associated stations, the text "No information available" is displayed.

The parameters shown are as follows:

- **MAC-Address**: Displays the MAC address of the station's radio.
- **Network**: States the name of the wireless network.
- **Device Name**: Shows the name of the station.
- **Last IP**: States the most recent IP address of the station as seen by the AP.
- **Signal**: Displays the received signal strength from the station, e.g., -31 dBm.
- **Signal/Chains**: Shows the received signal strengths from the station on each antenna, e.g., -52, -35, -34 dBm. The value of -95 dBm is taken to mean "no antenna" if the radio has only 2 antennas.
- **Noise**: Displays the received noise power at the AP.
- **TX Rate**: Shows the transmit bit rate from the AP towards this station.
- **RX Rate**: Shows the receive bit rate at the AP from this station.
- **TX-CCQ**: Indicates the wireless connection quality.

2.1.1.4 System

This **System** section shows the following information:

- **Router Name**: The name of the Access Point
- **Router Model**: The model of the Access Point
- **Firmware Version**: The AP's firmware version
- **Kernel Version**: The version of the kernel
- **Local Time**: Displays the local time

Figure 2-6: System Parameters

2.1.1.5 Memory

Here, the **Total Available** and **Free** memory are shown.

Figure 2-7: Total Available and Free Memory

2.1.1.6 Network

The **Network** section displays the status of the LAN and WAN networks.

Figure 2-8: Network Summary

- **Status**: Shows summaries of the interfaces for the LAN and WAN zones. This may include the following information:
  - Uptime
  - MAC address
  - Protocol
  - Bytes and packets received by the device
  - Bytes and packets transmitted by the device
  - IPv4 address.

2.1.1.7 DHCP Leases

The **DHCP Leases** section shows a table of MAC and IP addresses of connected computers with static DHCP leases. They are specified in the **Network > Interfaces > LAN > Static Leases** section of the device's configuration web page.

Figure 2-9: Currently Active Static DHCP Releases

2.1.1.8 Link Status (for Station Mode)

The **Link Status** section only applies if the device operates as an 802.11ac station.

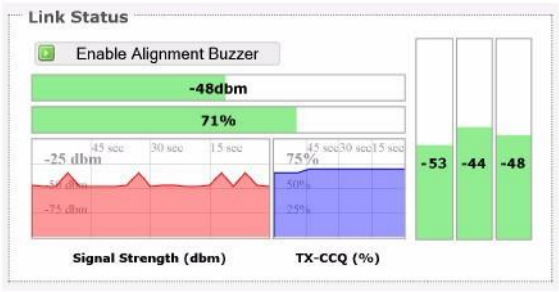

Figure 2-10: The Link Status Section

In the **Link Status** section on the **Status > Overview** web page, the value on the top left box denotes the current received signal strength, e.g., -48 dBm. The box directly below it shows the current TX-CCQ (transmission client connection quality), e.g., 71 %. The bottom left box shows a realtime graph of the received signal strength over the last 60 seconds. The box directly to its right shows a realtime graph of the TX-CCQ over the past 60 seconds.

On the right of this section, there are 3 vertical bars. Each bar shows the current received signal strength of each antenna, e.g., -53 dBm, -44 dBm, and -48 dBm. If the radio has only 2 antennas, the third vertical bar is given a default value of -95 dBm.

- **Enable Alignment Buzzer**: When enabled, the board would continually emit beeping sounds to indicate the received signal strength. Every 3 seconds, the board would emit a number of beeps (1 to 4) in quick succession. The number of beeps is the same as the number of lighted Signal strength indicator LEDs. Just like for LEDs, more beeps indicate a higher received signal strength. This is useful for a person aligning directional antennas at a height, in an outdoor scenario, if the LEDs are not visible. Another person on the ground could adjust the threshold values for the LEDs. There is some delay before the received signal strength gets reported by the alignment buzzer. To turn off the beeping sounds, click the **Disable Alignment Buzzer** button.

2.1.2 Routes

When you click on the **Status > Routes** tab; the routing rules that are currently active on the device are displayed.

Figure 2-11: The Status > Routes Page

- **ARP**: This address resolution protocol (ARP) table shows the IP address and corresponding MAC address of each device on the network.
- **Active IPv4-Routes**: This table shows the IPv4 gateway and network ID (Target) for each subnet.
- **Active IPv6-Routes**: This table shows the IPv6 gateway and network ID (Target) for each subnet.

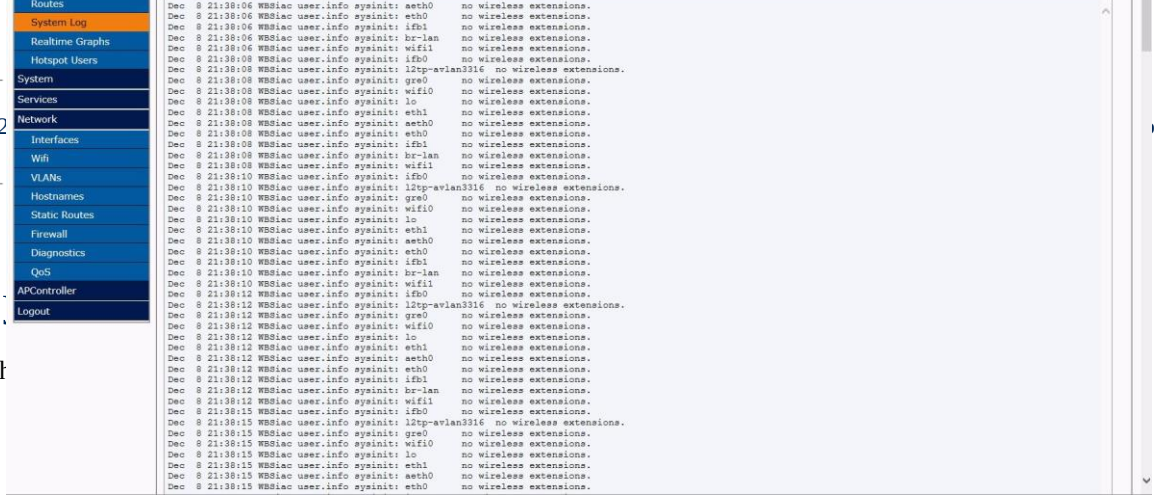

Figure 2-12: The System Log Page

2.1.4 Realtime Graphs

Under the tab for **Realtime Graphs**, there are four sub tabs titled as follows:

- Load
- Traffic
- Wireless
- Connections.

2.1.4.1 Lc

Figure 2-13: Realtime Load Graph

2.1.4.2 Traffic

You can display the following types of Realtime Traffic graphs:

- 2.4 GHz RF
- 5 GHz RF
- ath4
- LAN Bridge
- Right Port
- Left Port

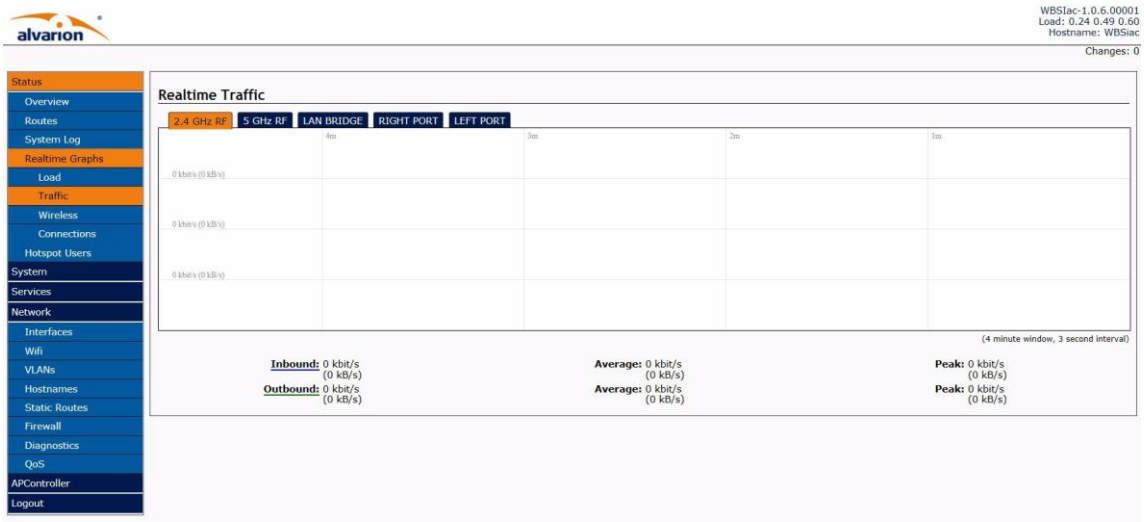

Figure 2-14: Realtime Load Graph - 2.4 GHz RF

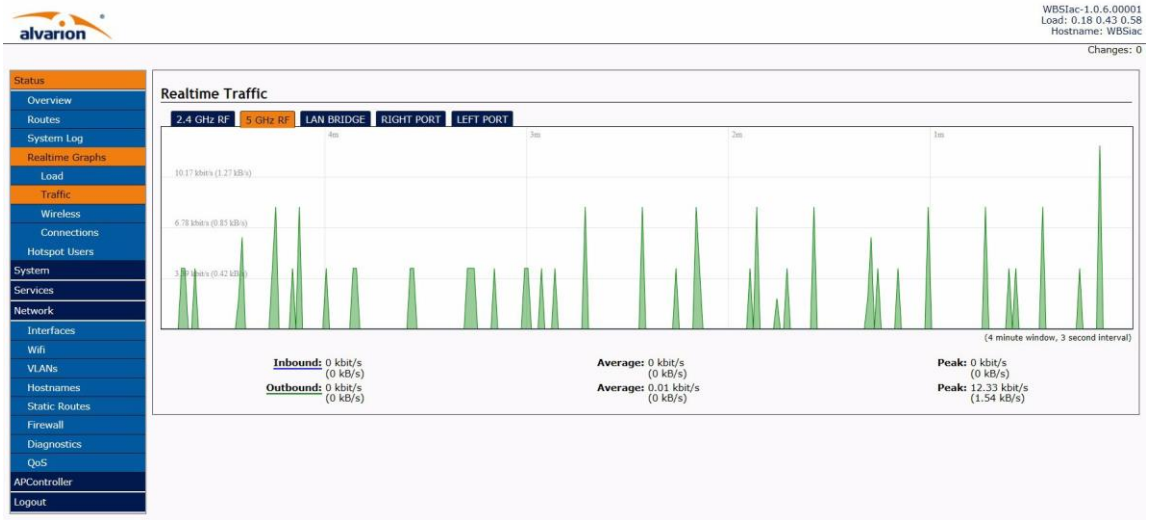

Figure 2-15: Realtime Load Graph - 5 GHz RF

Figure 2-16: Realtime Load Graph - LAN Bridge

Figure 2-17: Realtime Load Graph - Right Port

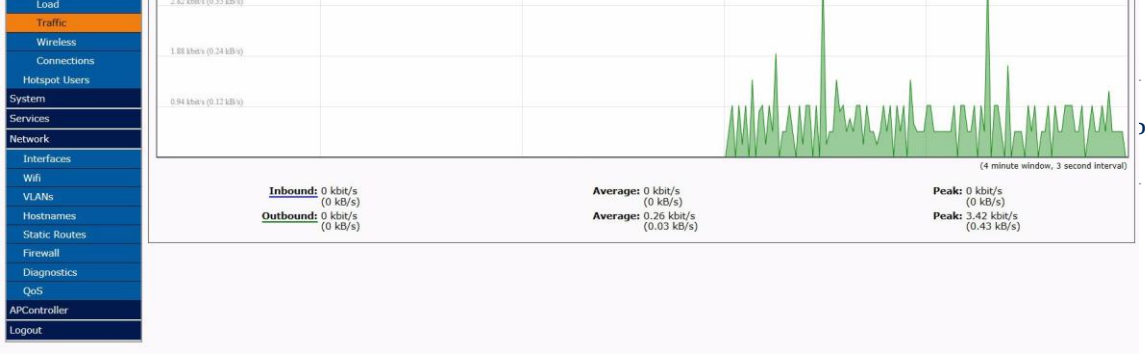

Figure 2-18: Realtime Load Graph - Left Port

2.1.4.3 Wireless

You can display the following types of Realtime Wireless graphs:

- 2.4 GHz RF
- 5 GHz RF
- ath4

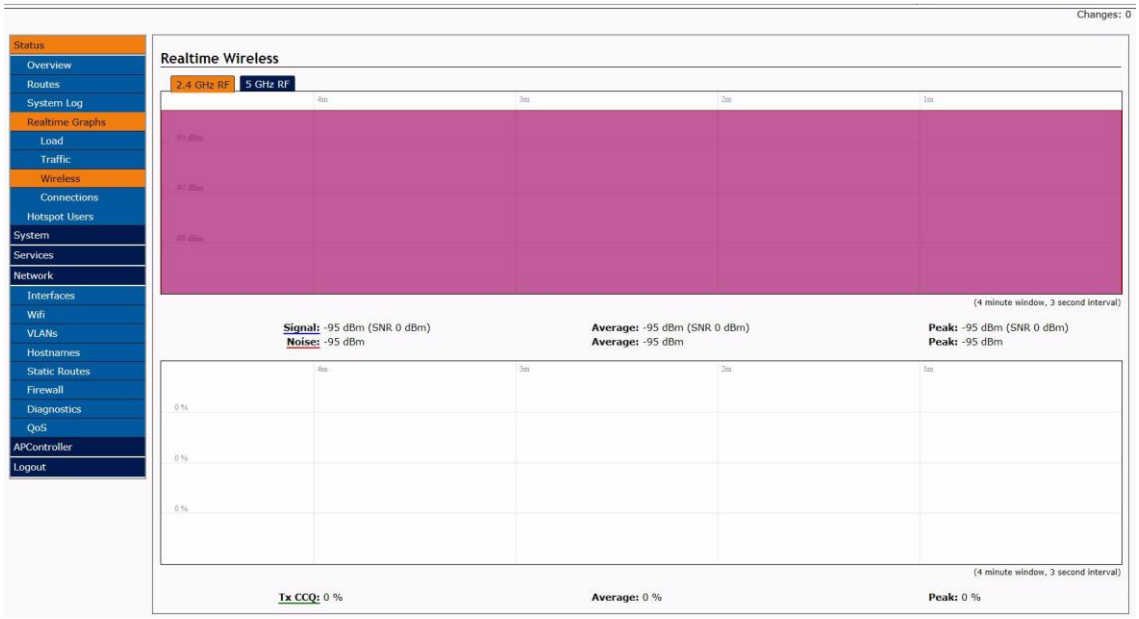

Figure 2-19: Realtime Wireless Graph - 2.4 GHz RF

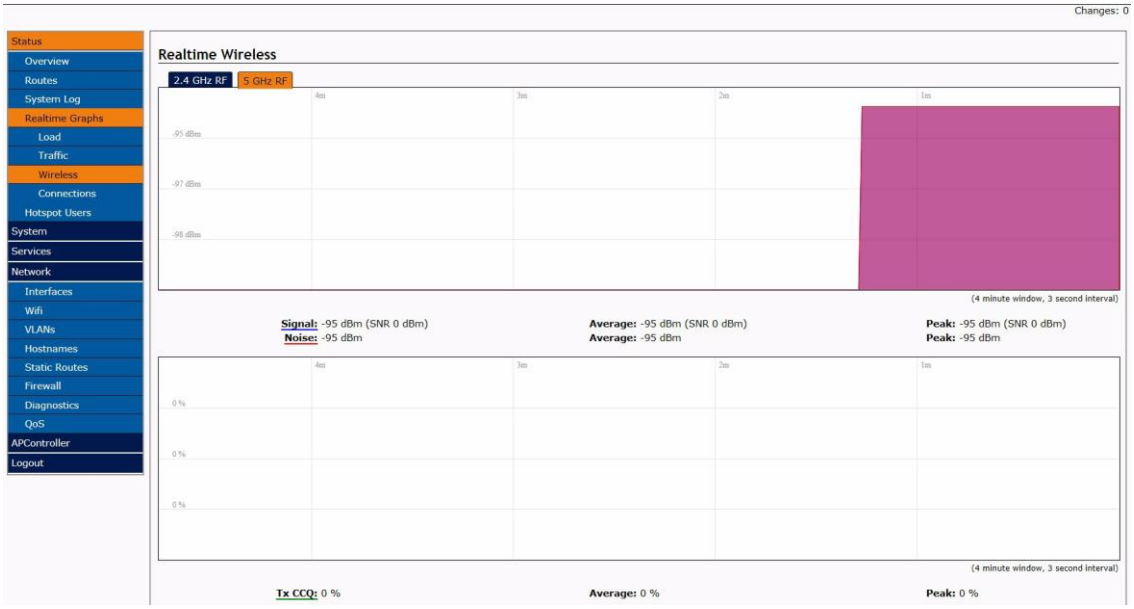

Figure 2-20: Realtime Wireless Graph - 5 GHz RF

Figure 2-21: Realtime Wireless Graph - ath4

Wireless
Connections
Hotspot Users
System
Services
Network
Interfaces
Wifi
VLANs
Hostnames
Static Routes
Firewall
Diagnostics
QoS
APController
Logout
(4 minute window, 3 second interval)
UDP: 14
TCP: 3
Other: 0
Average: 14
Average: 3
Average: 0
Peak: 15
Peak: 9
Peak: 0
IPV4 TCP 192.168.82.1:63282 WBSiac.lan:80 1.37 KB (22 Pkts.)
IPV4 TCP 192.168.82.1:63293 WBSiac.lan:80 1.33 KB (21 Pkts.)
IPV4 TCP 192.168.82.1:63296 WBSiac.lan:80 1.33 KB (21 Pkts.)
IPV4 UDP 131.168.1.2:42735 131.168.1.1:161 899.00 B (2 Pkts.)
IPV4 UDP 131.168.1.2:48651 131.168.1.1:161 899.00 B (2 Pkts.)
IPV4 UDP 131.168.1.2:51325 131.168.1.1:161 899.00 B (2 Pkts.)
IPV4 UDP 131.168.1.2:40428 131.168.1.1:161 426.00 B (2 Pkts.)
IPV4 UDP 131.168.1.2:42637 131.168.1.1:161 426.00 B (2 Pkts.)
IPV4 UDP 131.168.1.2:42256 131.168.1.1:161 377.00 B (2 Pkts.)
IPV4 UDP 131.168.1.2:48349 131.168.1.1:161 377.00 B (2 Pkts.)
IPV4 UDP 131.168.1.2:34830 131.168.1.1:161 377.00 B (2 Pkts.)
IPV4 UDP WBSiac.lan:20649 google-public-dns-a.google.com:53 70.00 B (1 Pkts.)
IPV4 UDP WBSiac.lan:20649 172.17.10.1:53 70.00 B (1 Pkts.)
IPV4 UDP WBSiac.lan:65183 google-public-dns-a.google.com:53 70.00 B (1 Pkts.)
IPV4 UDP WBSiac.lan:58479 google-public-dns-a.google.com:53 66.00 B (1 Pkts.)
IPV4 UDP WBSiac.lan:1701 10.10.226.98:1701 0.00 B (0 Pkts.)
IPV4 TCP 192.168.82.1:63299 WBSiac.lan:80 640.00 B (3 Pkts.)
IPV4 UDP 131.168.1.2:47700 131.168.1.1:161 426.00 B (2 Pkts.)
IPV4 TCP 192.168.82.1:63282 WBSiac.lan:80 1.37 KB (22 Pkts.)

Figure 2-22: Realtime Connections Graph

2.1.4.5 Hotspot Users

The Hotspot Users page shows the current online users and their status.

Figure 2-23: The Current Online Users and their Status

2.2 System Tab

This section is about the **System** top-level tab. Under this tab, the following sub tabs are available:

- System
- Administration
- Services
- SNMP
- Backup / Flash Firmware
- Reboot.

2.2.1 System

2.2.1.1 System Properties

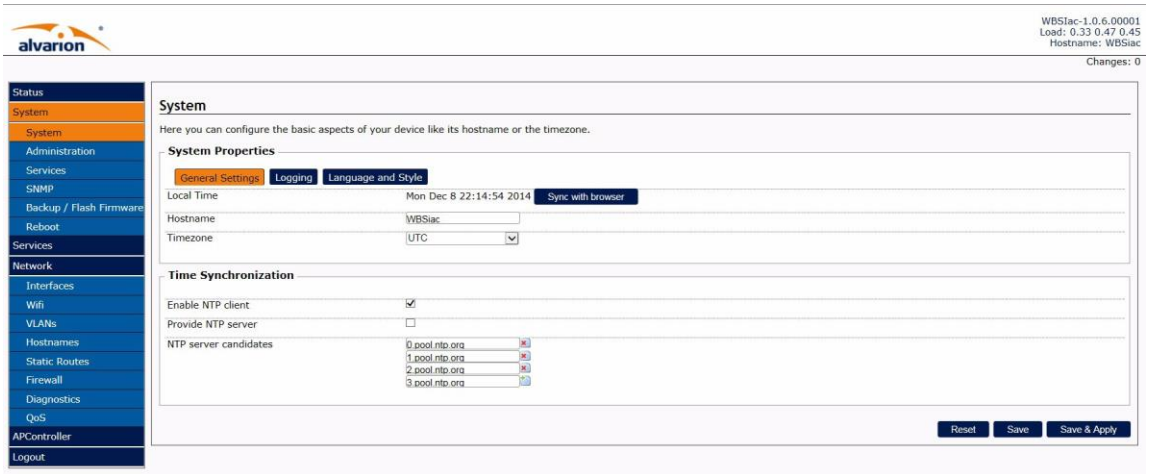

Figure 2-24: System Page

Within the **System** page, you can configure the device parameters such as the hostname and timezone.

The **System Properties** section includes the following tabs:

- General Settings
- Logging
- Language and Style.

2.2.1.1.1 General Settings

In the System Properties - General Settings tab, you can configure the following device parameters:

- **Local Time**: Displays the local time according to the Timezone.
- **Hostname**: Configures the name of the device.
- **Timezone**: Sets the timezone.

2.2.1.1.2 Logging

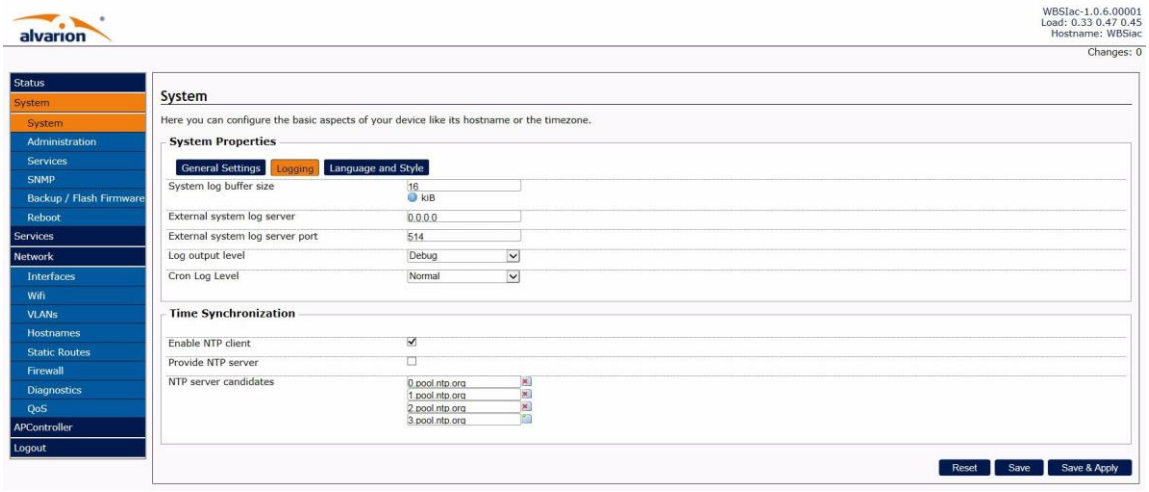

Figure 2-25: Logging

Logging specifies parameters used for the system log, such as:

- System log buffer size
- External system log server
- External system log server port
- Log output level
  - » Debug / Info / Notice / Warning / Error, Critical / Alert / Emergency
- Cron Log Level
  - » Debug / Normal / Warning

2.2.1.1.3 Language and Style

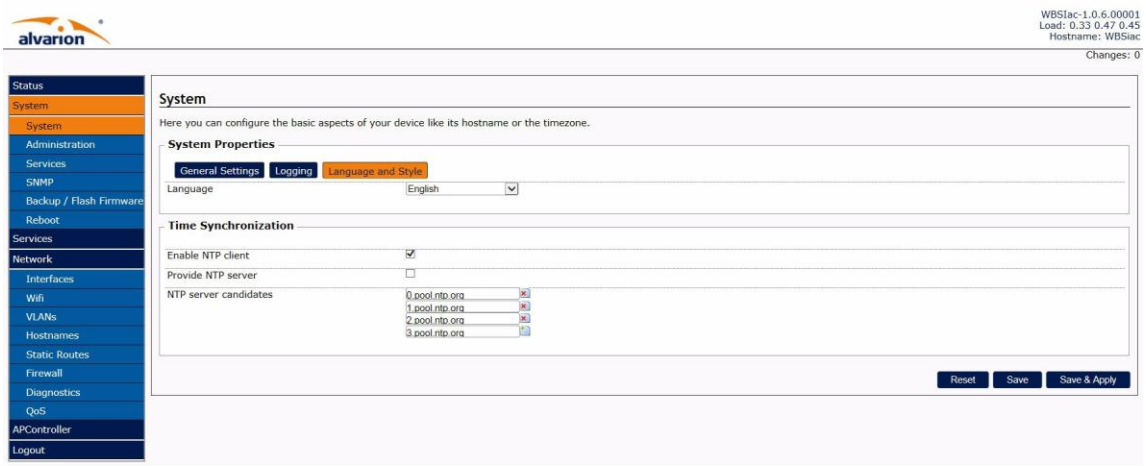

Figure 2-26: Language and Style

Language and Style allows you to choose the language and design of the WBSIac AP's web pages.

2.2.1.2 Time Synchronization

- **Enable NTP client**: Obtains the date and time from specified Network Time Protocol (NTP) servers.
- **Provide NTP server**: Click the checkbox option to provide an NTP server

Figure 2-27: Time Synchronization

2.2.2 Administration

Within the **System > Administration** page, you can configure the following settings:

- Router Password
- SSH
- Telnet
- Web.

2.2.2.1 Router Password

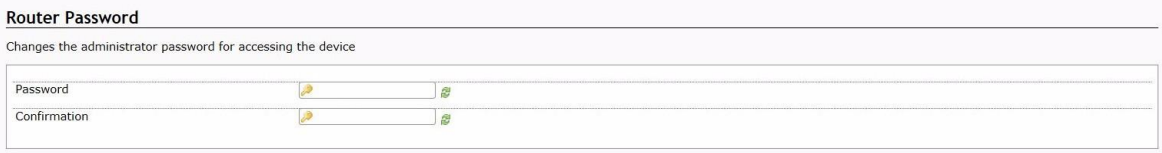

Figure 2-28: WBSIac AP Password

- **Password**: Allows you to set the WBSIac AP password, the default being password.
- **Confirmation**: Requires you to re-enter the password.

2.2.2.2 SSH

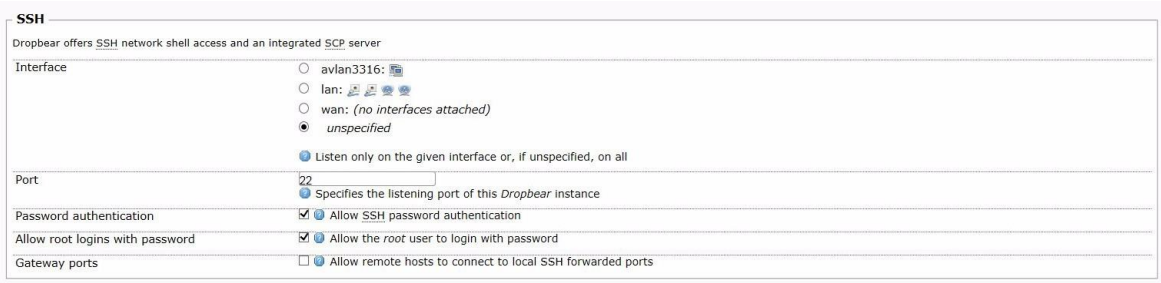
SSH
Dropbear offers SSH network shell access and an integrated SCP server
Interface
avlan3316:
lan:
wan: (no interfaces attached)
unspecified
Listen only on the given interface or, if unspecified, on all
Port
22
Specifies the listening port of this Dropbear instance
Password authentication
Allow SSH password authentication
Allow root logins with password
Allow the root user to login with password
Gateway ports
Allow remote hosts to connect to local SSH forwarded ports

Figure 2-29: SSH

SSH allows you to access the AP's Linux shell and file system using the Secure Shell protocol. For example, the programs PuTTY and WinSCP can be used.

- **Interface**: Lets the device listen on a given interface or all interfaces.
- **Port**: Specifies the listening port of the **Dropbear** instance, the default being 22.
- **Password authentication**: Allows SSH password authentication.
- **Allow root logins with password**: This is enabled by default.
- **Gateway ports**: Allow remote hosts to connect to local SSH forwarded ports.

2.2.2.3 Telnet

Figure 2-30: Telnet

- **Enable Telnet**: When enabled, it provides administrator tools for controlling the device or network debugging, over an unencrypted connection.
- **Port**: Specifies the listening port, the default being 23.

To start using Telnet, enter the command "telnet 192.168.1.1" or "telnet 192.168.1.1 23" into a Command Prompt when using Windows, or into a Terminal if using Linux or Mac OS X. This is assuming that 192.168.1.1 is the IP address of your AP.

The splash page of WBSIac appears after login. Commands can then be entered into the Linux shell of the AP, e.g., ifconfig, iwconfig, iwpriv, uci show, ls /bin, ls /sbin, ls /usr/bin, or ls /usr/sbin.

2.2.2.4 Web

Figure 2-31: Web

- **Web Server Mode**: This can be set to Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS).

  For HTTPS, if you see the warning, "The certificate is not trusted because it is self-signed. The certificate is only valid for WBSIac," click **Add Exception**, **Confirm Security Exception** and proceed.
- **Port**: Specifies the listening port, the default being 80 for HTTP and 443 for HTTPS.

2.2.3 Se

In t

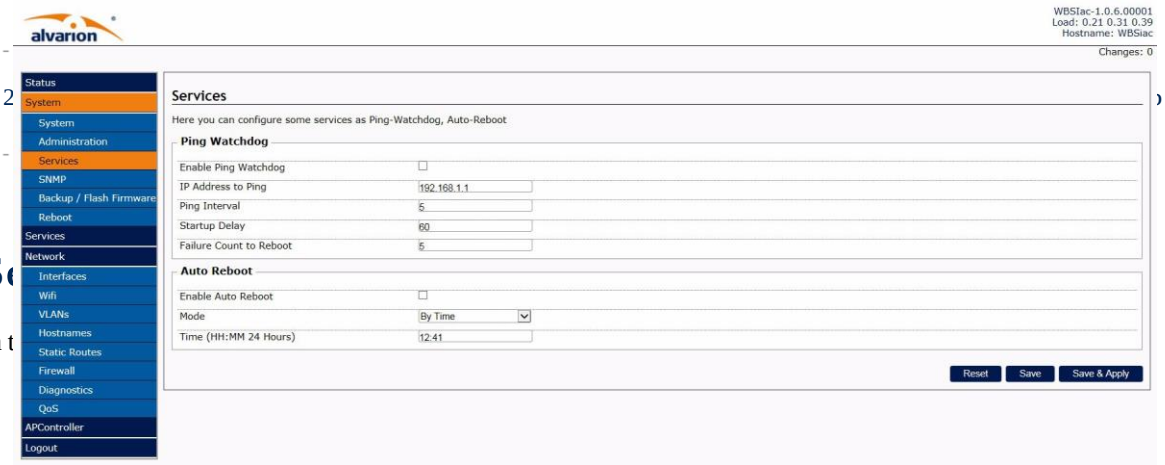

Figure 2-32: System > Services Page

2.2.3.1 Ping Watchdog

Figure 2-33: Ping Watchdog

- **Ping Watchdog**: Configures the device to ping to a remote IP address and reboot if the connection is lost. It is disabled by default.
- **IP Address to Ping**: Sets the remote IP address to ping, e.g., 192.168.1.10 or 8.8.8.8.
- **Ping Interval**: Specifies the time between successive pings, the default being 5 seconds.
- **Startup Delay**: Sets the time delay after the WBSlac AP finishes rebooting, before running the Ping Watchdog, the default being 60 seconds.
- **Failure Count to Reboot**: Specifies the number of failed pings before the WBSlac AP reboots automatically.

2.2.3.2 Auto Reboot

Figure 2-34: Auto Reboot

- **Auto Reboot**: Allows the WBSIac AP to reboot itself automatically, disabled by default.
- **Mode**: Chooses the Auto Reboot mode By Time or By Number of Hours.
- **Time (HH:MM 24 Hours)**: Sets the time of day to reboot if the Mode is By Time.

2.2.4 SNMP

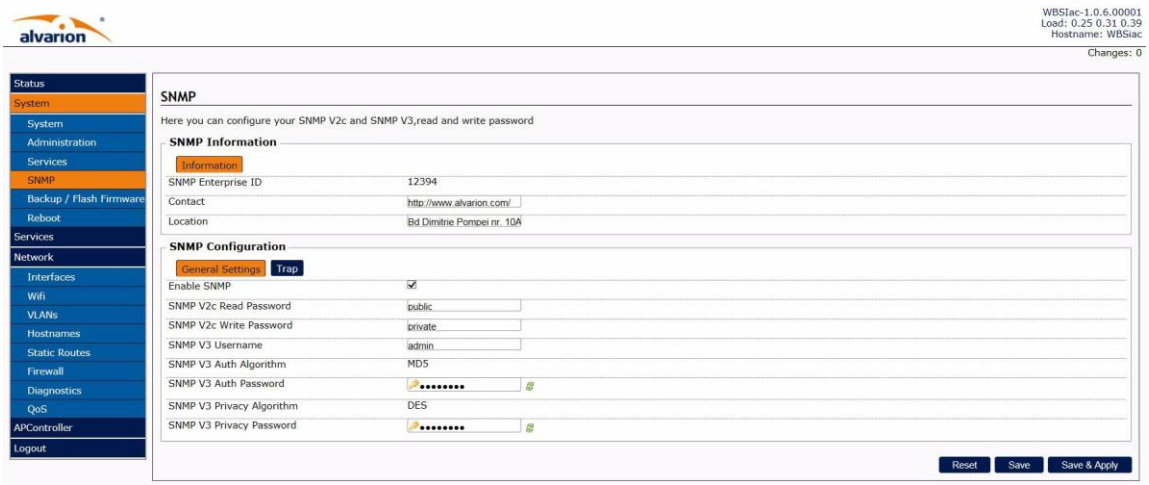

Figure 2-35: SNMP Page

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

In the **System > SNMP** page, you can configure SNMP V2c and SNMP V3 parameters.

2.2.4.1 SNMP Information

The following parameters are displayed in the **SNMP Information** section:

- SNMP Enterprise ID
- Contact

Figure 2-36: SNMP Information

2.2.4.2 SNMP Configuration

2.2.4.2.1 General Settings

Figure 2-37: SNMP Configuration - General Settings

- **Enable SNMP**: Enables SNMP.
- **SNMP V2c Read Password**: Sets the community string for read-only access (to the variables on the SNMP agent) by the network management station (NMS). The NMS is the software which runs on the SNMP manager, (default: public)
- **SNMP V2c Write Password**: Sets the community string for read-write access by the SNMP manager, (default: private)

  A community string identifies a group of SNMP agents. It is sent in clear text. It should be changed from the default string **public** or **private**. The variables on the SNMP agent can be classified into read-only or read-write variables.
- **SNMP V3 Username**: Sets the username for authentication (default: admin)
- **SNMP V3 Auth Algorithm**: Shows the authentication algorithm used, e.g., MD5.
- **SNMP V3 Auth Password**: Configures the password for user authentication (default: password)
- **SNMP V3 Privacy Algorithm**: Shows the data encryption algorithm used, e.g., DES.
- **SNMP V3 Privacy Password**: Sets the password for data encryption (default: password)

2.2.4.2.2 Trap

Figure 2-38: SNMP Configuration - Trap

- **Enable SNMP Trap**: Allows the SNMP agent to notify the SNMP manager of events.
- **SNMP Trap IP Address**: Sets the IP address of the SNMP manager which receives the trap messages.
- **SNMP Trap Port**: Sets the port number.

2.2.5 Physical Hardware Button

There is a physical button on the Access Point hardware board. Depending on how long the button is pressed, you can reboot the board or reset it to factory default. First, make sure then power is on. The following table shows the duration of the button press and the corresponding action.

Duration of button press	Action
0 - 3 seconds	Reboot
4 - 30 seconds	Reset to factory default
more than 30 seconds	Does nothing

2.2.6 Backup / Flash Firmware

The **System > Backup / Flash Firmware** page lets you perform backup and restore, or flash a new firmware.

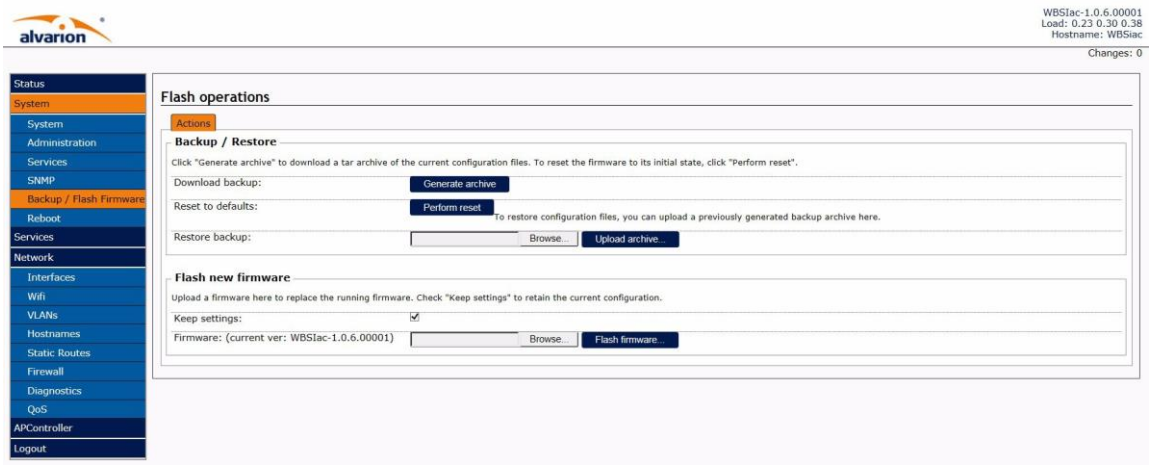

Figure 2-39: The System > Backup/Flash Firmware Page

The **System > Backup/Flash Firmware** page consists of the following sections:

- Backup / Restore
- Flash new firmware

2.2.6.1 Backup / Restore

Backup / Restore
Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset".
Download backup:
Generate archive
Reset to defaults:
Perform reset
To restore configuration files, you can upload a previously generated backup archive here.
Restore backup:
Browse...
Upload archive...

Figure 2-40: Backup / Restore

- **Download backup**: **Generate archive**: Downloads a tar archive of the current configuration files.

NOTE!

The backup archive file should be stored in a safe place because it contains the wireless password in clear text.

- **Reset to defaults**: **Perform reset**: Resets the firmware to its initial state.

NOTE!

If the radio card is changed from an 802.11ac card to a non-802.11ac card, perform a reset. This is because the configuration for the radio cards are different.

- **Restore backup**: **Upload archive**: Lets you upload a previously generated backup archive to restore configuration files.

2.2.6.2 Flash New Firmware

Flash new firmware
Upload a firmware here to replace the running firmware. Check "Keep settings" to retain the current configuration.
Keep settings:
Firmware: (current ver: WBSIac-1.0.6.00001)
Browse...
Flash firmware...

Figure 2-41: Flash New Firmware

You can upload a new firmware to replace the currently running firmware.

- **Keep settings**: Retains the current configuration.
- **Firmware**: Shows the current version of the firmware and allows you to upload a new firmware.

2.2.7 Reboot

Perform reboot: Reboots the operating system of your device. This is similar to the power-off and power-on cycle. The system configuration remains the same. Any changes that are not applied are lost.

2.3 Services Tab

The **Services** top-level tab contains the configuration pages for:

- Dynamic DNS
- Hotspot
- Discovery.

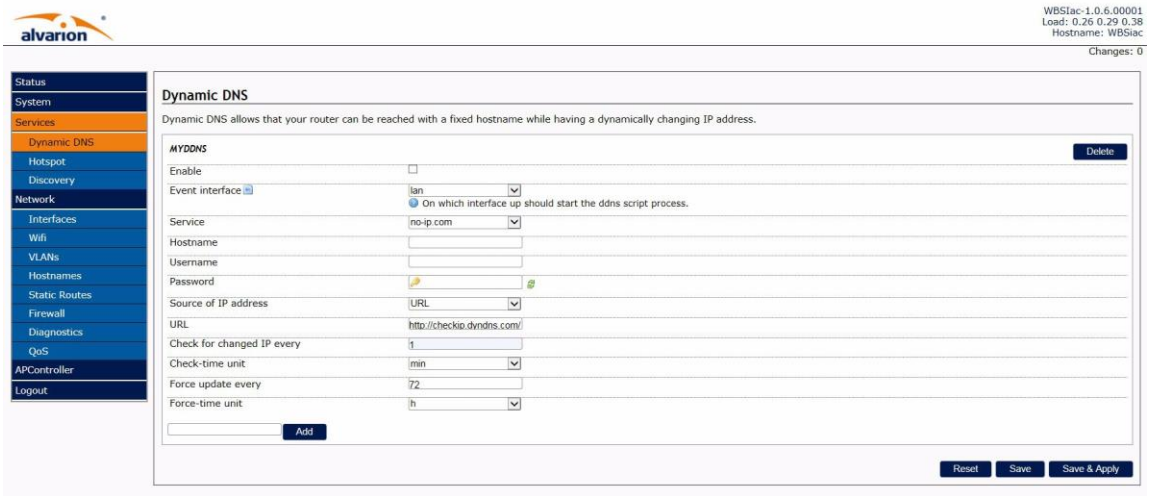

Figure 2-42: Services Tab

2.3.1 Dynamic DNS

The domain name system (DNS) translates a URL like www.yahoo.com to an IP address like 206.190.36.45. Dynamic DNS (DDNS) allows the WBSIac AP with the public IP address to be reached from the internet via a URL even if its IP address is dynamically changing.

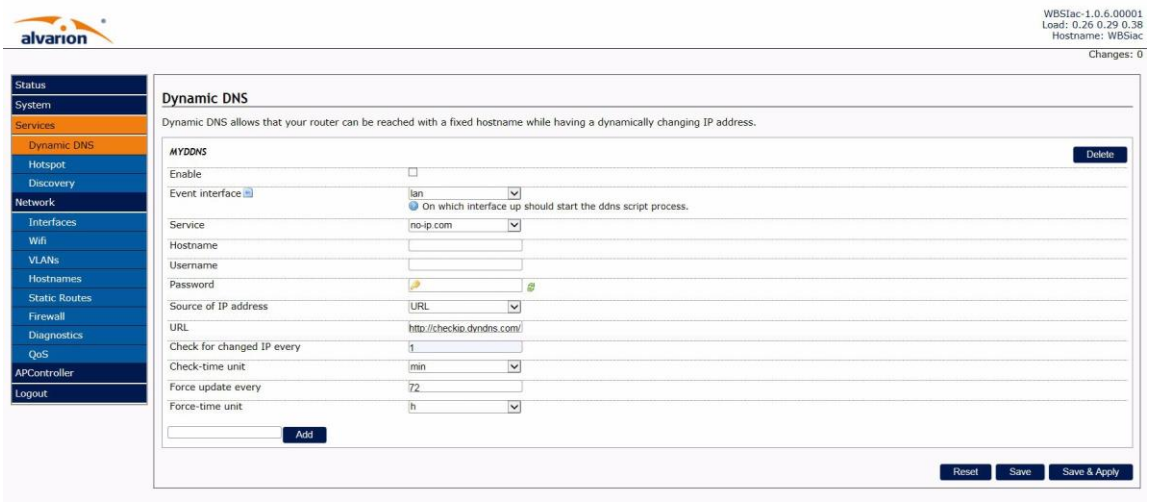

Figure 2-43: Dynamic DNS

- **Enable**: Enables the dynamic DNS.
- **Event interface**: Chooses the interface, e.g., LAN or WAN, for which "interface up" would run the DDNS script process.
- **Service**: Chooses the DDNS service provider, e.g., no-ip.com.
- **Hostname**: Specifies the hostname, e.g., y0033.no-ip.biz.
- **Username**: Sets the username registered for the DDNS service.
- **Password**: Sets the password registered for the DDNS service.
- **Source of IP Address**: Configures the source of the IP address information; the default is URL.
- **URL**: Sets the URL of the source of the IP address information, e.g., http://checkip.dyndns.com/.
- **Check for changed IP every**: The default is to check the IP address every 1 minute.
- **Check-time unit**: The default is **min** (minute).
- **Force update every**: The default is to force update every 72 hours.
- **Force-time unit**: The default is **h** (hour)

2.3.2 Hotspot

The Hotspot service allows you to control the access and usage of the Internet by connected devices.

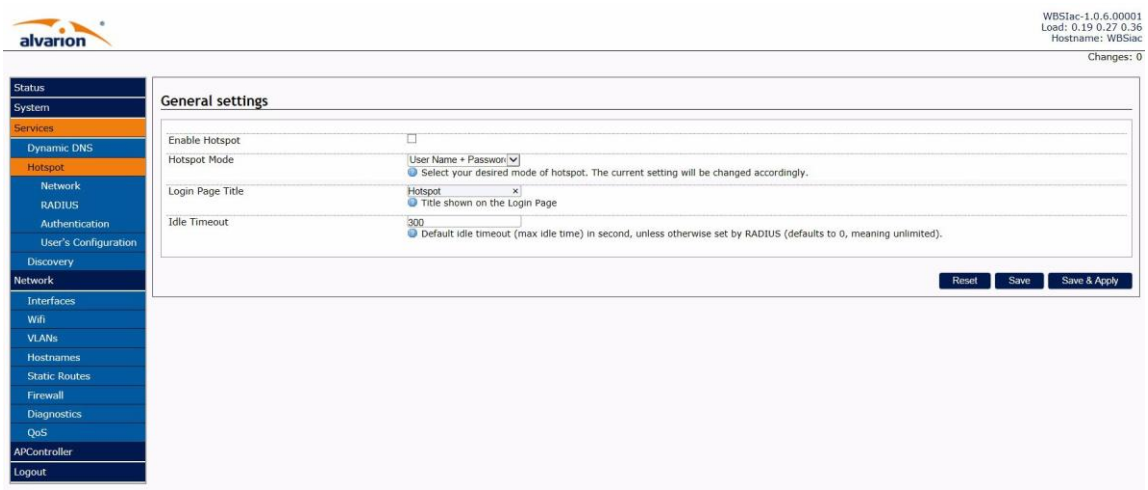

Figure 2-44: Hotspot

2.3.2.1 Setting up the Connections

The following subsections contain advice on configuring the WBSIac AP to implement the hotspot. The WBSIac AP is referred to here as the hotspot AP. It is recommended to configure the LAN, Wifi, and WAN, then test it before enabling the hotspot setting.

2.3.2.1.1 LAN Interface: DHCP Server

It is recommended to enable the DHCP server, because network address translation (NAT) occurs between the WAN zone and the LAN zone. To do this, you may go to the **Network** tab to disable the **Ignore interface** (Disable DHCP for this interface) option.

Devices or computers that connect to this hotspot AP can then obtain their IP addresses automatically. In addition, the default gateway IP address and the DNS server IP address are automatically configured for these connected devices.

If the DHCP server is left disabled, it is still possible for devices to connect to the hotspot. Each device would need a unique static IP address on the same subnet as this hotspot AP. Set the default gateway and DNS server for the device both to be the IP address of this hotspot AP.

It is not necessary to set the hotspot AP's default gateway and DNS server in the **Network** page. This information is obtained automatically from the WAN interface.

2.3.2.1.2 Wifi Settings

The wireless networks should be set up to allow any user to access the Internet, assuming that the hotspot is not yet enabled.

2.3.2.1.3 WAN Interface: Physical Settings

The hotspot has no effect if there is no WAN interface. To use the hotspot, set the WAN interface. The WAN interface should be the zone where the Internet access is available. It could be one of the Ethernet adapters or one of the wireless networks. All interfaces other than the WAN interface are considered as in the LAN zone. Any user in the LAN zone would see the hotspot login page after the hotspot is set up.

2.3.2.1.4 Test Internet Connection

At this point, before setting up the hotspot, it is good to test the Internet connection by connecting a mobile phone to a wireless network in the LAN zone of the hotspot AP.

The Internet browser may cache web pages, so to be sure, one may perform an Internet search of a random string of numbers. If the search results are returned, this means that the Internet connection is working fine.

2.3.2.2 Setting up the Hotspot

The hotspot can then be set up and enabled either by using the AP itself or by using the Arena Controller.

The following sections show the Hotspot settings available in the AP's web page.

2.3.2.3 General Settings

By clicking on the **Services** > **Hotspot** tab, the general settings are displayed.

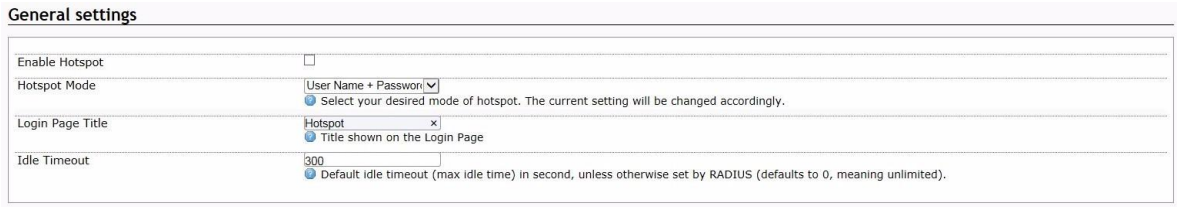
General settings
Enable Hotspot
Hotspot Mode
User Name + Passwor
Select your desired mode of hotspot. The current setting will be changed accordingly.
Login Page Title
Hotspot
Title shown on the Login Page
Idle Timeout
300
Default idle timeout (max idle time) in second, unless otherwise set by RADIUS (defaults to 0, meaning unlimited).

Figure 2-45: Hotspot General Settings

- **Enable Hotspot**: Turns on the hotspot service. You may wish to enable the hotspot after all the settings are completed.
- **Hotspot Mode**: Selects your required mode of hotspot. You can choose to use the hotspot together with a third party or external RADIUS authentication server.

NOTE!

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service.

The choices for the Hotspot Mode are:

- User Name + Password (Radius Required)
- Agreement (Radius Required)
- Password (Radius Required)
- Agreement (Radius not Required)
- Password (Radius not Required)

- **Login Page Title**: Sets the title shown on the Login Page, e.g., **HotSpot**.
- **Idle Timeout**: Configures the default idle timeout (max idle time) in seconds unless otherwise set by RADIUS (set as 0 to mean unlimited time).

2.3.2.4 Network Configuration

- **Network Parameters**
  - **Auto Config**: Automatically configures the network parameters. It is recommended to keep this enabled.

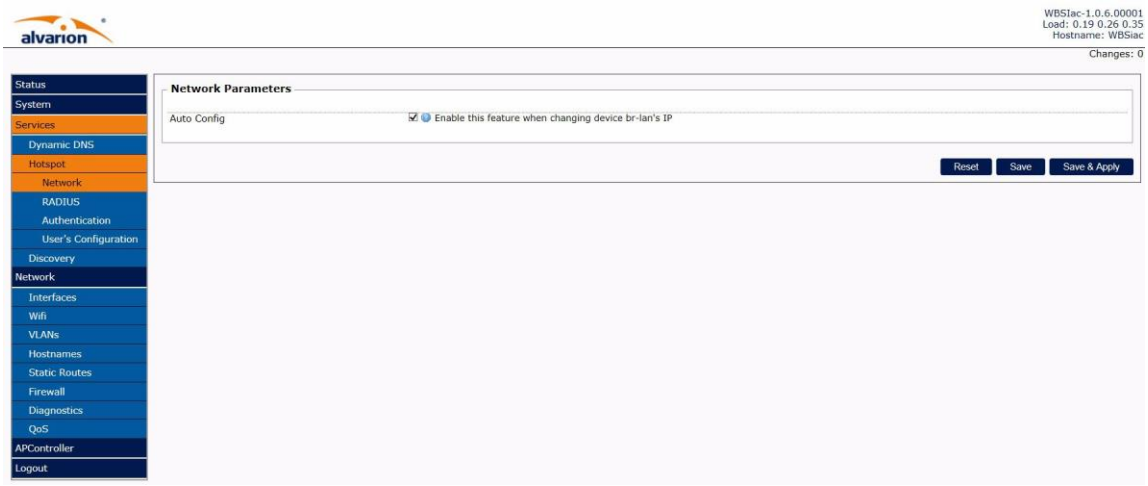

Figure 2-46: Network Parameters

2.3.2.5 RADIUS Configuration

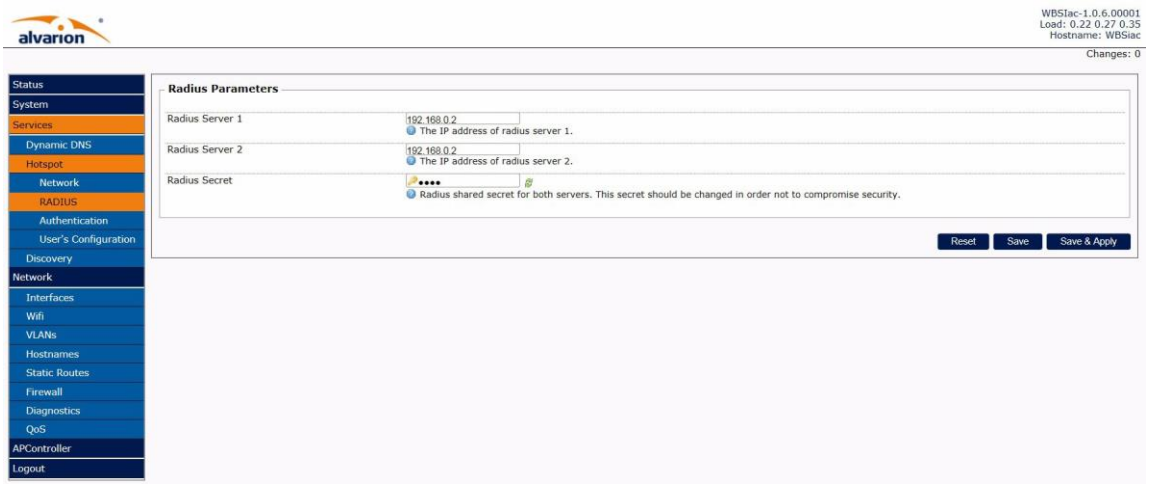

Figure 2-47: RADIUS Parameters

Here you can set the RADIUS parameters.

- **Radius Server 1**: Sets the IP address of Radius server 1, e.g.,127.0.0.1.
- **Radius Server 2**: Sets the IP address of Radius server, e.g., 127.0.0.1.
- **Radius Secret**: Sets the Radius shared secret for both servers. This secret should be changed in order not to compromise security.

2.3.2.6 Authentication

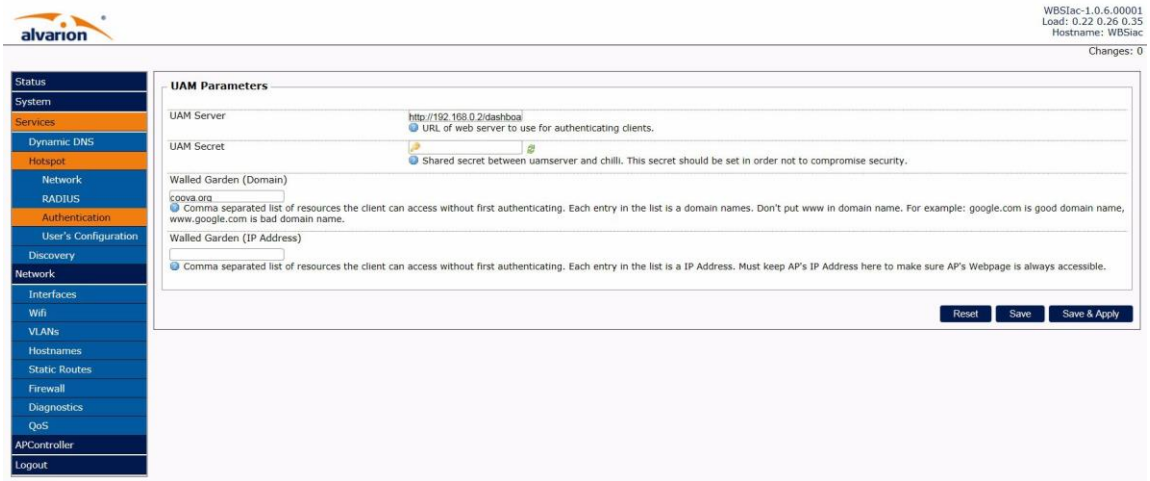

Figure 2-48: Authentication

Here you can set the Universal Access Method (UAM) parameters.

- **UAM Server**: Sets the URL of the web server to use for authenticating clients.

  For example: http://1.0.0.1/www/login.html

- **UAM Secret**: Configures the shared secret between uamserver and chilli. This secret should be set so as not to compromise security.

- **Walled Garden (Domain)**: Shows a comma separated list of resources the client can access without first having to authenticate. Each entry in the list is a domain name. Do not put www in the domain name. For example, "google.com" is a good domain name, "www.google.com" is not acceptable. The default is "coova.org".

- **Walled Garden (IP Address)**: Shows a comma separated list of resources the client can access without having to authenticate first. Each entry in the list is a IP Address. The AP's web page is always accessible.

2.3.2.7 User's Configuration

Here you can configure the users' network access and bandwidth limitations.

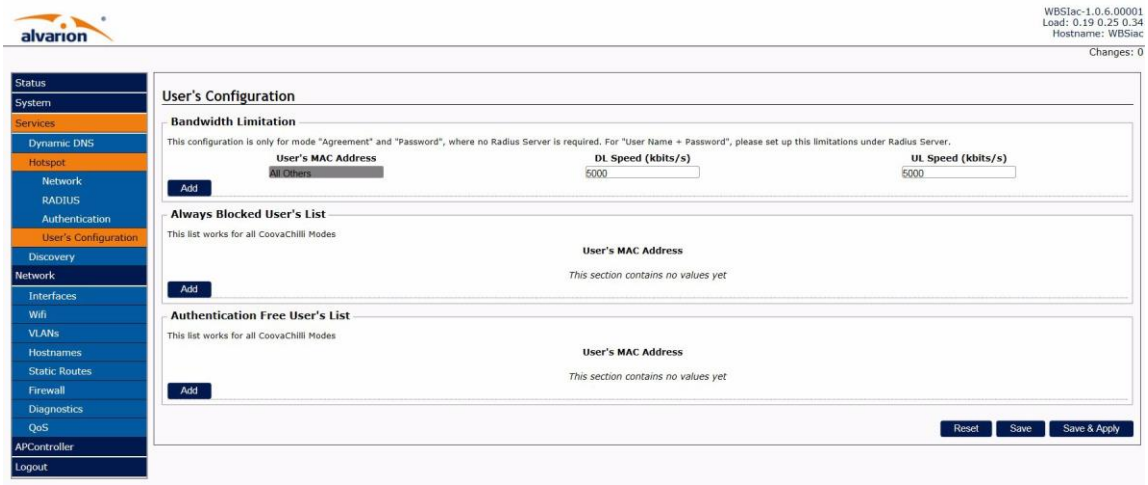

Figure 2-49: User's Configuration Page

2.3.2.7.1 Bandwidth Limitation

Bandwidth Limitation
This configuration is only for mode "Agreement" and "Password", where no Radius Server is required. For "User Name + Password", please set up this limitations under Radius Server.
User's MAC Address
DL Speed (kbits/s)
UL Speed (kbits/s)
All Others
5000
5000
Add

Figure 2-50: Bandwidth Limitation

This section only applies if the RADIUS Server is not required. If the RADIUS Server is required, this section is ignored.

You may add entries consisting of the following three fields:

- User's MAC Address
  - » Default entry: **All Others**
- Download (DL) Speed (kbits/s)
  - » Default entry: **5000**
- Upload (UL) Speed (kbits/s)
  - » Default entry: **5000**

This means that all hotspot users are subjected to 5000 kbits/s bandwidth limitation. To prevent any limitation, it may be set to a high value like 5000000 kbits/s.

2.3.2.7.2 Always Blocked User's List

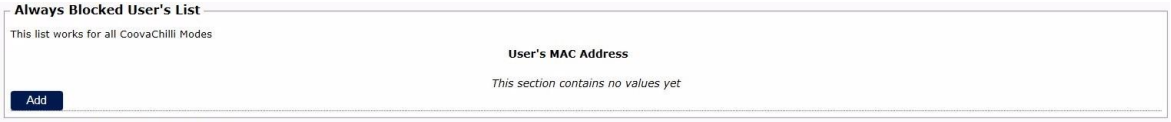
Always Blocked User's List
This list works for all CoovaChilli Modes
User's MAC Address
This section contains no values yet
Add

Figure 2-51: Always Blocked User's List

You may add entries for **User's MAC Address**.

These users would be blocked from accessing the network.

This list works for all Hotspot modes.

2.3.2.7.3 Authentication Free User's List

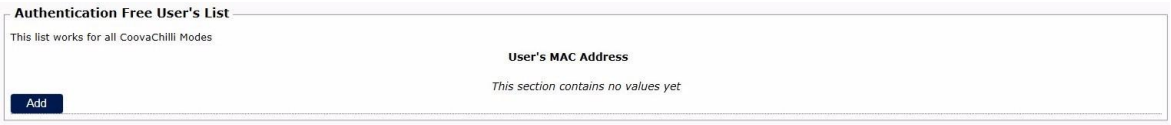
Authentication Free User's List
This list works for all CoovaChilli Modes
User's MAC Address
This section contains no values yet
Add

Figure 2-52: Authentication Free User's List

You may add entries for **User's MAC Address**.

These users would not need any authentication at all and can get immediate access to the network. For example, the boss of the company could be in the authentication free list.

This list works for all Hotspot Modes.

2.3.2.8 Logging-in to the Hotspot

When a hotspot user opens an Internet browser on the computer, it would automatically show the hotspot login page. To quickly see the hotspot login page, the user could enter a simple URL in the Internet browser, e.g.,

- 1.0.0.1
- 8.8.8.8
- bing.com

When a user connects the mobile/smart phone to the hotspot wireless network, the hotspot login page should automatically appear. Otherwise, the user could open the default Internet browser app or Chrome app on their mobile phone to see the login page.

2.3.2.9 Possible Hotspot Scenarios

The WAN interface could be set as one of the Ethernet ports. This means that the wireless networks provided by the hotspot AP would be in the LAN zone. Users can connect within the LAN zone to see the hotspot login page.

The wireless distribution system (WDS) can also be used to increase the coverage. More information is found in Section 2.4.5.2 Interface Configuration.

2.3.3 Discovery

Figure 2-53: Discovery

- **Enable**: Allows the Device Name and Last IP address of the wireless station to be discovered by the wireless access point. The functionality is similar to the Cisco Discovery Protocol. Discovery is enabled by default.

2.4 Network Tab

The **Network > Interfaces** tab shows an overview of the network interfaces. You can view and configure the interfaces of the local area network (LAN) zone as well as the wide area network (WAN) zone. Network address translation (NAT) occurs between these two network zones. The AP that performs the NAT is called a gateway. A gateway is a network point that acts as an entrance to another network.

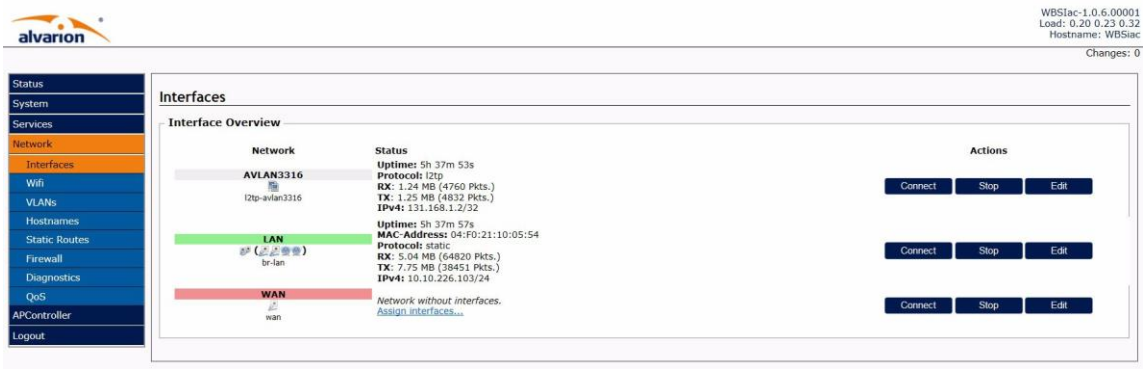

Figure 2-54: Network > Interfaces Page

Figure 2-55: Interface Overview

The Network column shows that the WAN zone has the physical port **wan** as its interface.

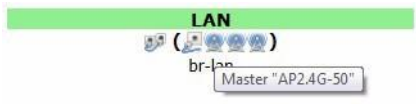

Figure 2-56: Infotip

An infotip is displayed when hovering the mouse over the icon.

In Figure 2-56, the LAN zone (icon with four Ethernet ports) has the bridged interface "br-lan" which consists of one physical port (icon with two Ethernet port) and two wireless networks (each icon looking like a short standing fan) on the device. Hovering the mouse over each icon would give the name of the

interface it represents. In this example, the infotip shows that there is a (virtual) access point on the device with "M78" as its network name.

2.4.1 Interfaces - WAN

The **Network > Interfaces > WAN** page configures the interface for the WAN zone.

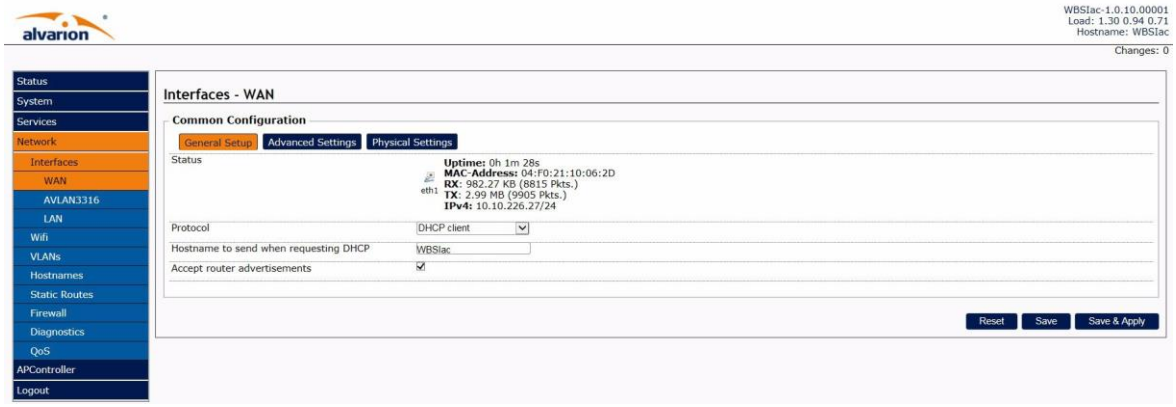

Figure 2-57: Common Configuration for the WAN Zone

2.4.1.1 Common Configuration

2.4.1.1.1 General Setup

- **Status**: Shows a summary of the interface for the WAN zone. This includes the following:
  - **Uptime**
  - **MAC Address**
  - **RX**: Bytes and packets received by the device
  - **TX**: Bytes and packets transmitted by the device
  - **IPv4** address.

Figure 2-58: General Setup for the WAN Zone

- **Protocol**: Select from the following choices where the device should obtain its IP address automatically:

  - **Static address**: Where you can specify the device IP address

    - **IPv4 address**: Sets the IP address of the device as seen from the WAN zone.
    - **IPv4 netmask**: Sets the subnet mask, e.g., 255.255.255.0. The IP address and netmask together determine the subnet or network ID, e.g., 192.168.3.0/24. Two devices must be in the same subnet in order to establish a (Layer 2) link between them.
    - **IPv4 gateway**: Specifies the IP address of the remote AP that allows the device's shell to gain internet access.
    - **IPv4 broadcast**: Specifies the IPv4 broadcast address, optional.
    - **Use custom DNS servers**: Configures the IP address of the DNS servers, e.g., 165.21.100.88 for the SingNet DNS server or 8.8.8.8 for the Google DNS server. The computers in the same subnet as this device can then set this device's IP address as their preferred DNS server to obtain the same DNS service.

  - **DHCP Client**: (default)

    The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used by servers on an IP network to allocate IP addresses automatically to client devices.

    - **Hostname to send when requesting DHCP**: Specifies the name of this device as seen by the remote DHCP server.

  - **PPTP**

    The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over Transmission Control Protocol (TCP) and a Generic Routing Encapsulation (GRE) tunnel operating to encapsulate Point-to-Point Protocol (PPP) packets.

    - **VPN Server**: Specifies the IP address of the remote PPTP server for the virtual private network (VPN).
    - **PAP/CHAP username**: Sets the username for the Password Authentication Protocol (PAP) or the Challenge-Handshake Authentication Protocol (CHAP).
    - **PAP/CHAP password**: Sets the password for the PAP or CHAP.
    - **Configure PPTP IP settings**: Upon clicking the "Configure..." button, the PPTP Common Configuration page would be displayed. The protocol DHCP client or Static address can be selected. The corresponding options are explained within this section (Section 2.4.1.1 Common Configuration).

» **PPPoE**

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames. Most DSL providers use PPPoE, which provides authentication, encryption, and compression.

The options PAP/CHAP username and PAP/CHAP password have been explained earlier.

- **Access Concentrator**: Identifies the PPPoE server. Leave empty to autodetect.
- **Service Name**: Specifies the PPPoE service name. The server accepts clients which send an initialization message with the service name that matches the server's configuration. Leave empty to autodetect.

» **L2TP**

The Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

The options PAP/CHAP username and PAP/CHAP password have been explained earlier.

- **L2TP Server**: Specifies the IP address of the remote L2TP server.
- **Configure L2TP IP settings**: Upon clicking the "Configure..." button, the L2TP Common Configuration page would be displayed. The protocol DHCP client or Static address can be selected. The corresponding options are explained within this section (Section 2.4.1.1 Common Configuration).

2.4.1.1.2 Advanced Settings

The following are options in the **Advanced Settings** section tab. Thee options that are displayed depends on the protocol that is used.

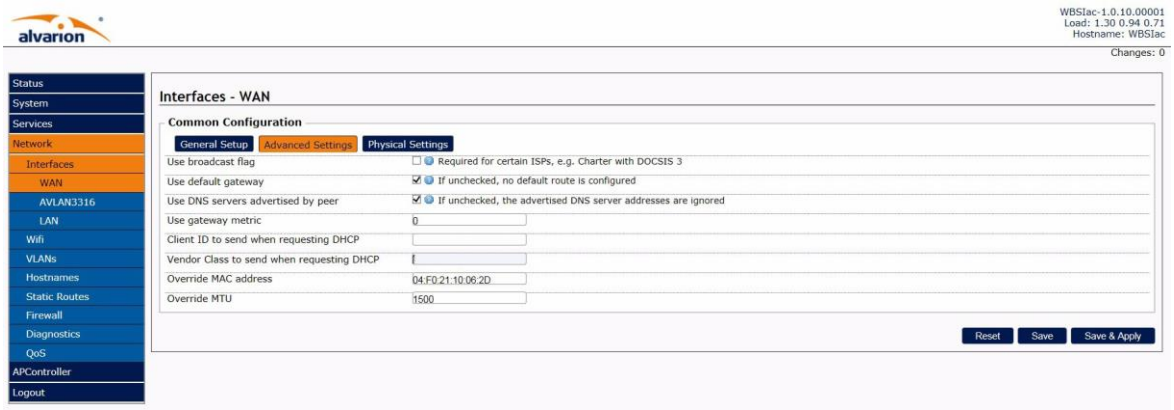

Figure 2-59: WAN Zone - Advance Settings

- **Use broadcast flag**: When sending DHCP requests, a client can indicate if it wants an answer in unicast or broadcast, by setting the broadcast flag. This is required for certain ISPs. Unchecked by default.
- **Use default gateway**: Configures a default route. Checked by default.
- **Use DNS servers advertised by peer**: Uses the DNS settings advertised by the DHCP server. Checked by default.
- **Use gateway metric**: Allows you to specify a gateway metric. This acts as a cost for choosing the gateway when a connected device has to select between multiple available gateways. The gateway with the smallest metric is chosen.
- **Client ID to send when requesting DHCP**: Sets the identifier that may be required by the ISP or network administrator. If not stated, the MAC address of the client will be sent.
- **Vendor Class to send when requesting DHCP**: Identifies the vendor of a DHCP client for the enhancement of vendor-specific DHCP functionality.
- **Override MAC address**: Allows you to specify a different MAC address other than the AP's original MAC address. This is useful if the ISP uses the MAC address of the AP to identify a customer. Suppose that the AP needs to be replaced. The new AP can take on the MAC address of the previous AP in order to continue having internet access.
- **Override MTU**: Sets the maximum transmission unit (MTU), the default being 1500 bytes. Unless, your ISP requires, it is not recommended to change this setting.

The following options are specific to the PPTP and PPPoE protocols:

- **LCP echo failure threshold**: Sets the number of link control protocol (LCP) echo failures before the peer is presumed to be dead. Use 0 to ignore failures.
- **LCP echo interval**: Specifies the interval in seconds to send LCP echo requests. This is only effective in conjunction with failure threshold.
- **Inactivity timeout**: Sets the number of seconds of inactivity, after which the connection is closed. Use 0 to persist connection.

2.4.1.1.3 Physical Settings

- **Interface**: Chooses which physical interface to use for the WAN zone. This can be the Ethernet Adapter "eth0" or "eth1" that corresponds to each of the two ports on the device for example. It could also be set as the Wireless Network. If No Interface is selected, all interfaces would be within the LAN zone.

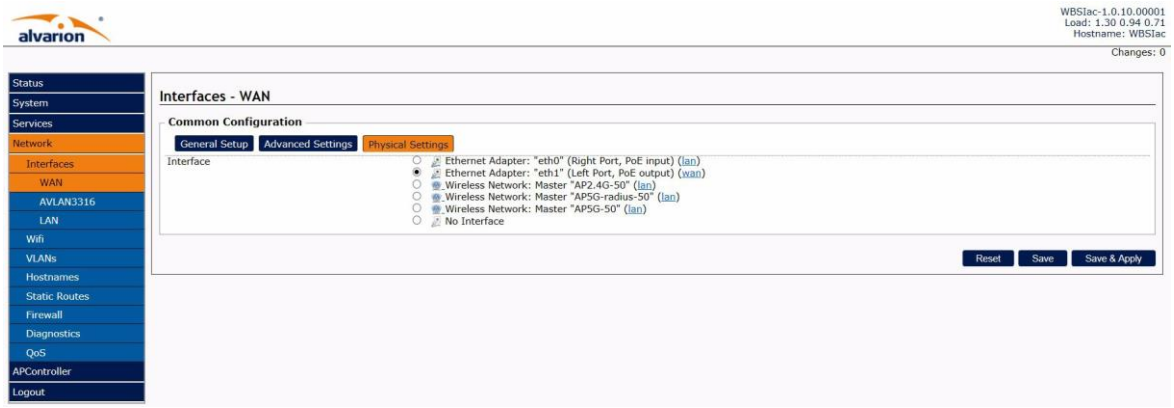

Figure 2-60: WAN Zone - Physical Settings

NOTE!

For boards with 2 ethernet ports, both ports would be LAN ports in the default configuration. You can still designate the WAN port in the firmware. For APs with power over Ethernet (PoE), only the port further away from the DC Jack (right port) would be the PoE input port (ethY). The port nearer to the DC Jack (left port) would be the PoE output port (ethX).

2.4.2 Interfaces - AVLAN3316

2.4.2.1 Common Configuration

2.4.2.1.1 General Setup

Figure 2-61: AVLAN3316 Common Configuration

- Status
- Protocol
  - Static Address
  - DHCP Client
- Really Switch Protocol?
  - Switch Protocol button

2.4.3 Interfaces - LAN

The LAN interface consists of the following sections:

- Common Configuration
- DHCP Server
- Static Leases.

2.4.3.1 Common Configuration

The LAN interface Common Configuration section has the following tabs:

- General Setup
- Advanced Settings
- Physical Settings

2.4.3.1.1 General Setup

- **Status**: Shows a summary of the current LAN port status, which includes:
  - **Uptime**
  - **MAC Address**
  - **RX**: Received bytes and packets
  - **TX**: Transmitted bytes and packets
  - **IPv4** address.

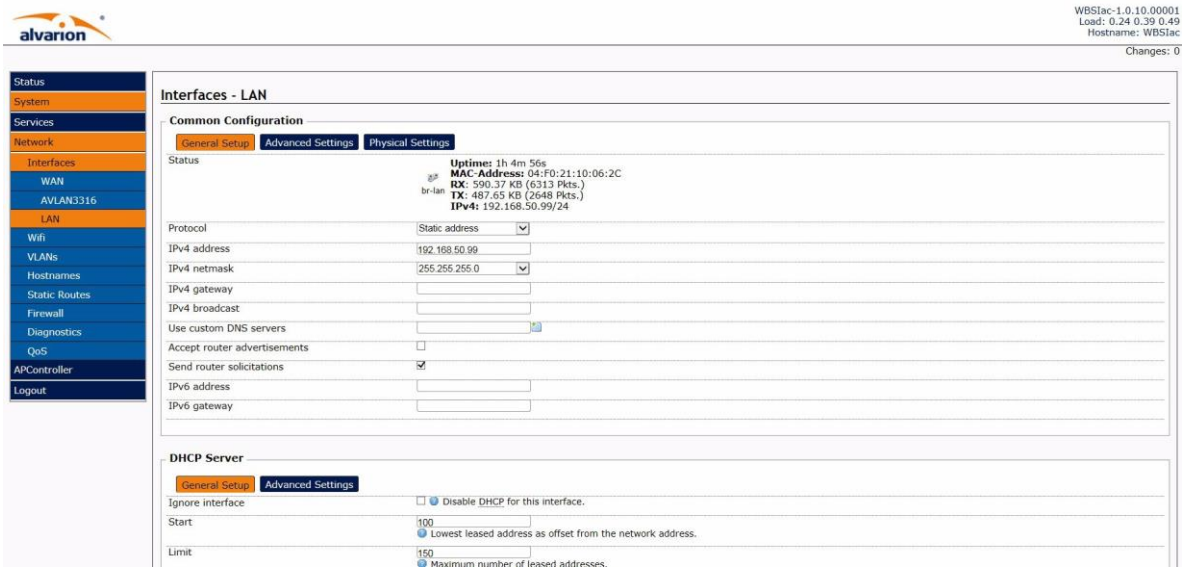

Figure 2-62: LAN Zone - General Setup

- **Protocol**: Chooses between Static address, where you can specify the device IP address, or DHCP client, where the device obtains it IP address automatically. Static address is necessary if other devices obtain internet connection through this device. Static address is also recommended if you wish to configure the device via the web interface.

  - **Static Address**

  - **DHCP Client**: The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used by servers on an IP network to allocate IP addresses automatically to client devices.

    Hostname to send when requesting DHCP: Specifies the name of this device as seen by the remote DHCP server.

- **IPv4 address**: Sets the IP address of the device, e.g., 192.168.21.1, where you can access the AP's configuration web page.

- **IPv4 netmask**: Sets the subnet mask, e.g., 255.255.255.0. The IP address and netmask together determine the subnet or network ID, e.g., 192.168.21.0/24. Two devices must be in the same subnet in order to establish a (Layer 2) link between them.

- **IPv4 gateway**: Specifies the IP address of the remote AP that allows the device's shell to gain internet access.

- **IPv4 broadcast**: Specifies the IPv4 broadcast address, optional.

- **Use custom DNS servers**: Configures the IP address of the DNS servers, e.g., 165.21.100.88 for the SingNet DNS server or 8.8.8.8 for the Google DNS server. The computers in the same subnet as this device can then set this device's IP address as their preferred DNS server to obtain the same DNS service.

- **Accept router advertisements**: Checkbox option unchecked by default

- **Send router solicitations**: Checkbox option checked by default
- **IPv6 address**
- **IPv6 gateway**

2.4.3.1.2 Advanced Settings

The following are options in the **Advanced Settings** section tab. The options displayed depends on the protocol being used.

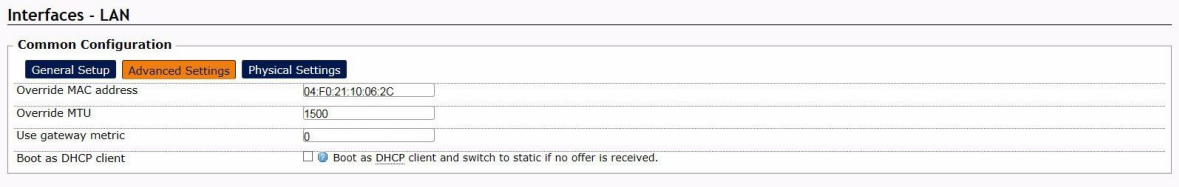

Figure 2-63: LAN Zone - Advanced Settings

- **Override MAC address**: Allows you to specify a different MAC address other than the AP's original MAC address. This is useful if the ISP uses the MAC address of a AP to identify a customer. Suppose that the AP needs to be replaced. The new AP can take on the MAC address of the previous AP in order to continue having internet access.
- **Override MTU**: Sets the maximum transmission unit (MTU), the default being 1500 bytes. Unless, your ISP requires, it is not recommended to change this setting.
- **Use gateway metric**: Allows you to specify a gateway metric. This acts as a cost for choosing the gateway when a connected device has to select between multiple available gateways. The gateway with the smallest metric is chosen.
- **Boot as DHCP client**: Boot as DHCP client and switch to static if no offer is received.
- Use broadcast flag: When sending DHCP requests, a client can indicate if it wants an answer in unicast or broadcast, by setting the broadcast flag. This is required for certain ISPs. Unchecked by default.
- Use default gateway: Configures a default route. Checked by default.
- Use DNS servers advertised by peer: Uses the DNS settings advertised by the DHCP server. Checked by default.
- Client ID to send when requesting DHCP: Sets the identifier that may be required by the ISP or network administrator. If not stated, the MAC address of the client will be sent.
- Vendor Class to send when requesting DHCP: Identifies the vendor of a DHCP client for the enhancement of vendor-specific DHCP functionality.

2.4.3.1.3 Physical Settings

- **Enable STP**: Enables the Spanning Tree Protocol on this bridge. It is unchecked by default.

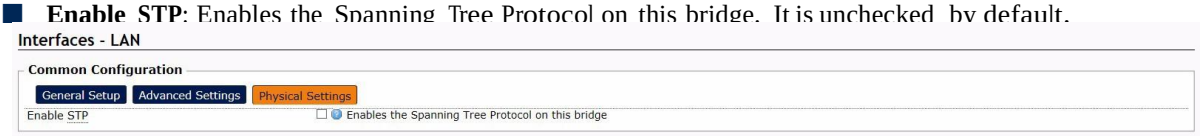

Figure 2-64: LAN - Physical Settings

2.4.3.2 DHCP Server

This section allows you to configure the device as a DHCP server.

2.4.3.2.1 General Setup

- **Ignore interface**: Disables DHCP for this interface. You should uncheck this to enable DHCP.

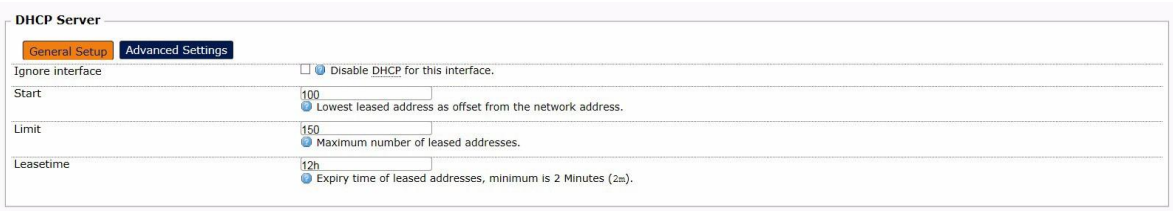

Figure 2-65: LAN - DHCP Server - General Setup

NOTE! All the following options in this DHCP Server section depend on DHCP being enabled.

- **Start**: Specifies the lowest leased address as offset from the network address, the default being 100.
- **Limit**: Sets the maximum number of leased addresses, the default being 150.
- **Leasetime**: States the expiry time of leased addresses, the default being 12h.

2.4.3.2.2 Advanced Settings

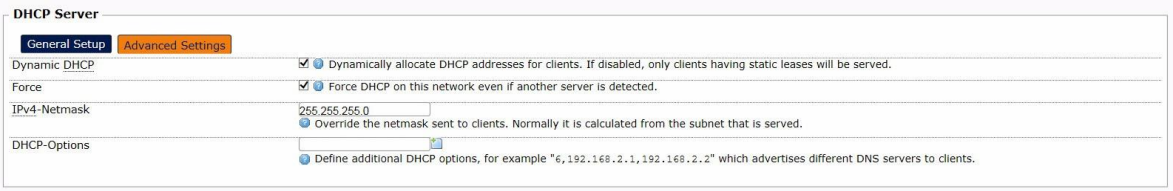
DHCP Server
General Setup
Advanced Settings
Dynamic DHCP
Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
Force
Force DHCP on this network even if another server is detected.
IPv4-Netmask
255.255.255.0
Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
DHCP-Options
Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

Figure 2-66: LAN - DHCP Server - Advanced Settings

- **Dynamic DHCP**: Dynamically allocates DHCP addresses for clients. If disabled, only clients having static leases are served. Checked by default.
- **Force**: Forces DHCP on this network even if another server is detected, unchecked by default.
- **IPv4-Netmask**: Overrides the netmask sent to clients. Normally it is calculated from the subnet that is served.
- **DHCP-Options**: Defines additional DHCP options, for example "6,192.168.2.1, 192.168.2.2" which advertises different DNS servers to clients. Normally, connected devices would take this board's IP address as the default gateway. To set an alternative default gateway, add the DHCP option "3,192.168.2.3" for example.

2.4.3.3 Static Leases

In this section, you can specify that a particular DHCP client obtain an IP address that you define. The MAC address of the client is required.

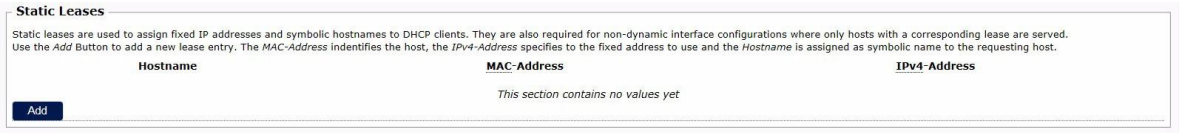
Static Leases
Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.
Use the Add Button to add a new lease entry. The MAC-Address indentifies the host, the IPv4-Address specifies to the fixed address to use and the Hostname is assigned as symbolic name to the requesting host.
Hostname
MAC-Address
IPv4-Address
This section contains no values yet
Add

Figure 2-67: LAN - Static Leases

Click the **Add** button to add a static DHCP lease, then click **Save & Apply** to apply the changes.

Static Leases
Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.
Use the Add Button to add a new lease entry. The MAC-Address indentifies the host, the IPv4-Address specifies to the fixed address to use and the Hostname is assigned as symbolic name to the requesting host.
Hostname
MAC-Address
IPv4-Address
Delete
Add
Reset
Save
Save & Apply

Figure 2-68: Adding a Static Lease

The static DHCP lease shows up on the **Status > Overview** page if the client is active.

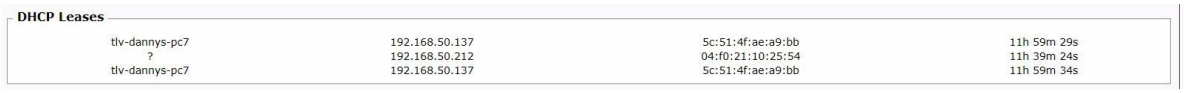

Figure 2-69: Static DHCP Lease

2.4.4 Wifi - Overview

Clicking on the **Network > Wifi** tab would bring you to the **Wireless Overview** page. This page shows the radios present on the device. These may include the on-board radio and the miniPCI/miniPCIe radio card. The wireless local area networks (WLANs) are displayed under each radio.

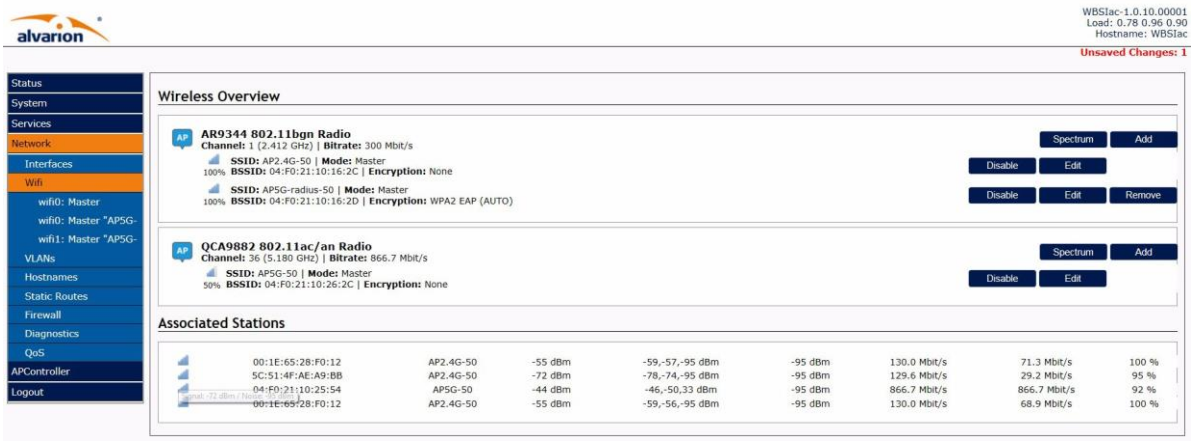

Figure 2-70: Wireless Overview

In Figure 2-70, two tabs are shown at the top. They correspond to the its two radios shown.

The buttons are explained as follows.

- **Spectrum**: Shows the Channel Scan Report and allows you to run the Interference Analyzer.
- **Add**: Allows you to add virtual access points (VAPs) to the radio. By default, there is only one VAP on the radio. Each VAP corresponds to one network.
- **Enable**: Enables the radio.
- **Disable**: Disables the radio.
- **Edit**: Brings you to the configuration page of the network. Clicking this button is equivalent to clicking the corresponding tab above, e.g., wifi1: Master "M7" for the radio with SSID given as "M7".
- **Remove**: Removes the radio.

2.4.4.1 Radio in AP Mode

When a radio is operating as an AP, the section for **Associated Stations** shows a list of stations connected to this device.

Figure 2-71: Associated Stations

The following Associated Station details are displayed:

- MAC address
- Network name
- Received signal strength
- Noise power
- Transmit rate
- Receive rate
- Transmission quality for each station are displayed.

2.4.4.2 Spectrum: Interference Analyzer

For a radio in AP mode, clicking the **Spectrum** button would bring up the Channel Scan Report.

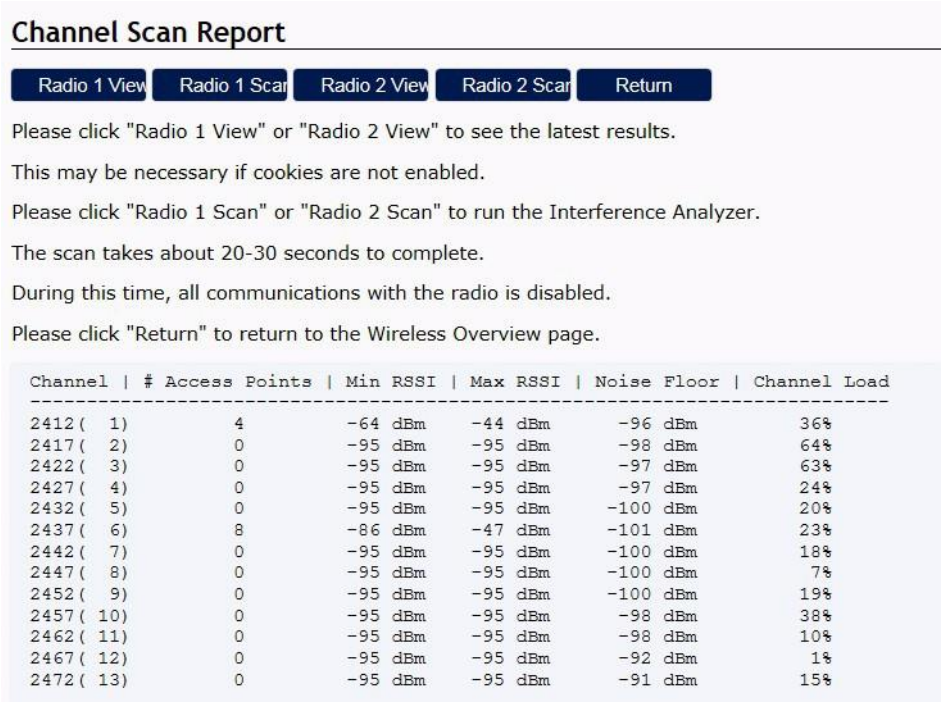
Channel Scan Report
Radio 1 View
Radio 1 Scan
Radio 2 View
Radio 2 Scan
Return
Please click "Radio 1 View" or "Radio 2 View" to see the latest results.
This may be necessary if cookies are not enabled.
Please click "Radio 1 Scan" or "Radio 2 Scan" to run the Interference Analyzer.
The scan takes about 20-30 seconds to complete.
During this time, all communications with the radio is disabled.
Please click "Return" to return to the Wireless Overview page.
Channel | # Access Points | Min RSSI | Max RSSI | Noise Floor | Channel Load
2412(1) 4 -64 dBm -44 dBm -96 dBm 36%
2417(2) 0 -95 dBm -95 dBm -98 dBm 64%
2422(3) 0 -95 dBm -95 dBm -97 dBm 63%
2427(4) 0 -95 dBm -95 dBm -97 dBm 24%
2432(5) 0 -95 dBm -95 dBm -100 dBm 20%
2437(6) 8 -86 dBm -47 dBm -101 dBm 23%
2442(7) 0 -95 dBm -95 dBm -100 dBm 18%
2447(8) 0 -95 dBm -95 dBm -100 dBm 7%
2452(9) 0 -95 dBm -95 dBm -100 dBm 19%
2457(10) 0 -95 dBm -95 dBm -98 dBm 38%
2462(11) 0 -95 dBm -95 dBm -98 dBm 10%
2467(12) 0 -95 dBm -95 dBm -92 dBm 1%
2472(13) 0 -95 dBm -95 dBm -91 dBm 15%

Figure 2-72: The Channel Scan Report

The **Radio 1 View** button shows the number of neighboring access points for each channel, the Min RSSI, Max RSSI, Noise Floor, and Channel Load.

- **Min RSSI:** Shows the minimum received signal strength indicator due to the neighboring access points.
- **Max RSSI**: Shows the maximum received signal strength indicator due to the neighboring access points.
- **Noise Floor**: Shows the level of the noise on the channel.
- **Channel Load**: Shows how much the channel is utilized. A lower channel load denotes a channel with less interference.

You can click **Radio 1 Scan** to do the full channel scan again and get the latest results.

The buttons for Radio 2 would be shown if Radio 2 is enabled on the device.

- **Return**: Brings you back to the **Wireless Overview** page.

Channel	# Access Points	Min RSSI	Max RSSI	Noise Floor	Channel Load
2412(1)	4	-48 dBm	-27 dBm	-97 dBm	11%
2417(2)	1	-72 dBm	-72 dBm	-97 dBm	26%
2422(3)	0	-95 dBm	-95 dBm	-98 dBm	32%
2427(4)	0	-95 dBm	-95 dBm	-97 dBm	15%
2432(5)	0	-95 dBm	-95 dBm	-99 dBm	16%
2437(6)	7	-71 dBm	-32 dBm	-100 dBm	19%
2442(7)	0	-95 dBm	-95 dBm	-101 dBm	13%
2447(8)	0	-95 dBm	-95 dBm	-100 dBm	6%
2452(9)	0	-95 dBm	-95 dBm	-100 dBm	5%
2457(10)	0	-95 dBm	-95 dBm	-97 dBm	6%
2462(11)	0	-95 dBm	-95 dBm	-98 dBm	6%
2467(12)	0	-95 dBm	-95 dBm	-92 dBm	1%
2472(13)	0	-95 dBm	-95 dBm	-91 dBm	7%

Figure 2-73: A Channel Scan Report for the 5 GHz Band

2.4.4.3 Radio in Station Mode

A radio can operate as a Station. This can be set in the Interface **Configuration > General Setup > Mode** option, after clicking on the **Edit** button.

Figure 2-74: The Wireless Overview Page Showing a Radio as a Client (Station)

The following buttons are for a radio operating as a station.

- **Scan**: Scans for available wireless networks. This button is available if the device is operating as a Station. You can then select the network to connect to.
- **Join Network**: Associates this device with the selected wireless network.

2.4.5 Wifi - Wireless Network

As mentioned earlier, clicking on the **Edit** button for a network would bring you to the configuration page. This page contains the sections **Device Configuration** and **Interface Configuration**.

The **Device Configuration** section covers the physical settings of the radio hardware such as channel, transmit power, or antenna selection. These are shared among all defined wireless networks of the radio. Per network settings like encryption or operation mode are grouped in the Interface Configuration.

2.4.5.1 Device Configuration

The Device Configuration section consists of the section tabs for **General Setup** and **Advanced Settings**.

2.4.5.1.1 General Setup

- **Status**: Shows a summary of the wireless network.

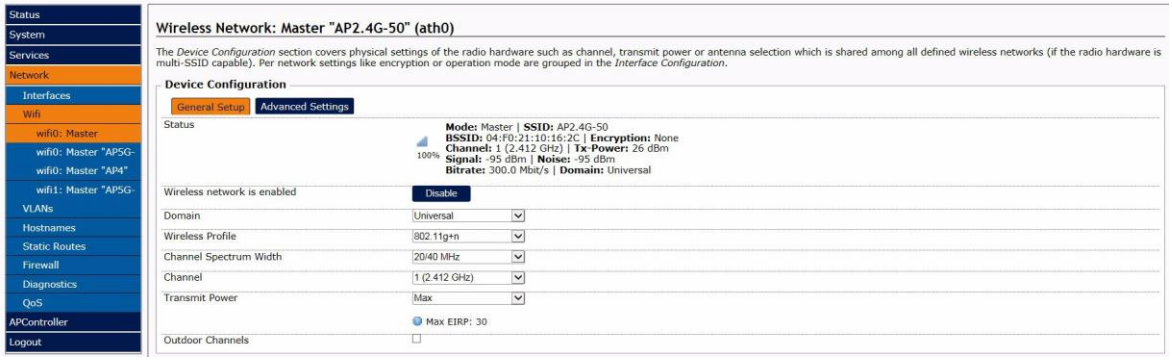

Figure 2-75: Wifi Device Configuration

- **Wireless network is enabled/disabled**
  - » **Enable**: Enables the wireless network.
  - » **Disable**: Disables the wireless network.
- **Domain**
  - » **Universal**
- **Wireless Profile**: Chooses the wireless standard used. 802.11ac and 802.11g are older standards while 802.11n is a newer standard that offers higher data rates. The choice of **802.11g+n** is a combination of 802.11g and 802.11n, and operates in the 2.4 GHz frequency band. The choice of 802.11a+n is a combination of 802.11ac and 802.11n, and operates in the 5 GHz frequency band. The 802.11ac is the latest standard that offers even higher data rates (up to 1300 Mbps) and it also operates in the 5 GHz frequency band.

- **Channel Spectrum Width**: Selects whether **20 MHz** or **20/40 MHz** bands are used. A 40 MHz band has twice the throughput of a 20 MHz band. A smaller bandwidth may allow more devices to be connected. The 20/40 MHz option allows both 20 and 40 MHz bands to be used. When the 802.11ac wireless standard is used, the 20/40/80 MHz band can be selected. An 80 MHz band can carry twice the amount of data of a 40 MHz band.
- **Channel**: Chooses the frequency channel. The default setting of **Auto** may be used. For an AP, it would select the channel with the least interference from other APs. For a station, it would automatically select the same channel as its AP. The frequency channel may also be manually selected. An AP and its station must have the same channel in order to communicate.
  - Auto
  - 1 (2.412 GHz)
  - 2 (2.417 GHz)
  - 3 (2.422 GHz)
  - 4 (2.427 GHz)
  - 5 (2.432 GHz)
  - 6 (2.437 GHz)
  - 7 (2.442 GHz)
  - 8 (2.447 GHz)
  - 9 (2.452 GHz)
  - 10 (2.457 GHz)
  - 11 (2.462 GHz)
  - 12 (2.467 GHz)
  - 13 (2.472 GHz)
- **Transmit Power**: Chooses the transmit power of the radio, e.g., 4 dBm, 5 dBm, 6 dBm, ... up to 26 dBm or Max. This is the total power supplied to the antennas of the radio. The maximum power also depends on the frequency channel used.
- **Outdoor Channels**: Limits the available channel frequency selections to 5500-5700 MHz if the country is in the European Union (EU). Based on the EU-Rule 2005/513/EC regulation, only this frequency band is allowed for outdoor use.
- Country Code: Selects the country. Each country has its own transmit power and frequency regulations. To ensure regulatory compliance, you must select the country where the device is operating in. The transmit power levels for each channel are tuned accordingly.

- Obey Regulatory Power: Obeys the power regulations specified by each country. This would satisfy the legally permitted maximum for the equivalent isotropically radiated power (EIRP) limits of the selected country, based on the specified Antenna Gain (dBi). The result is that the maximum transmit power may be less than the capability of the radio. Once activated, a refresh of the web page may be needed to show the settings correctly.
- Antenna Gain (dBi): Represents the gain relative to an isotropic antenna. A higher antenna gain results in the transmit power more focused towards a certain direction. When Obey Regulatory Power is checked, the value of the antenna gain would be taken into account to limit the selectable transmit power, such that the EIRP limits of the country are satisfied.

2.4.5.1.2 Advanced Settings

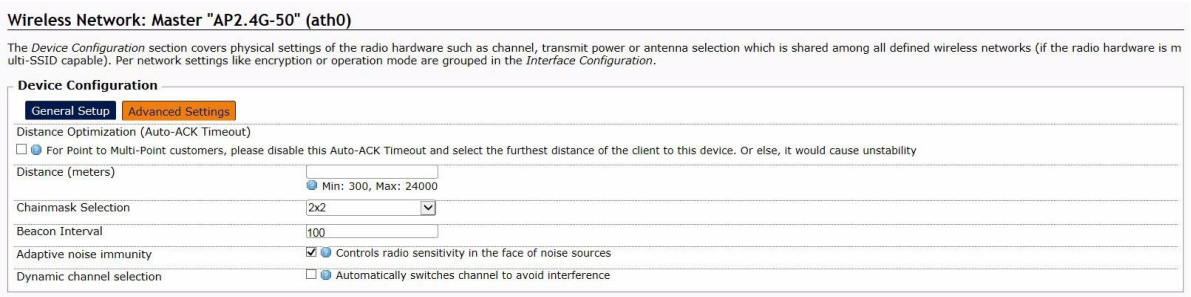
Wireless Network: Master "AP2.4G-50" (ath0)
The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which is shared among all defined wireless networks (if the radio hardware is m
ulti-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.
Device Configuration
General Setup
Advanced Settings
Distance Optimization (Auto-ACK Timeout)
For Point to Multi-Point customers, please disable this Auto-ACK Timeout and select the furthest distance of the client to this device. Or else, it would cause unstability
Distance (meters)
Min: 300, Max: 24000
Chainmask Selection
2x2
Beacon Interval
100
Adaptive noise immunity
Controls radio sensitivity in the face of noise sources
Dynamic channel selection
Automatically switches channel to avoid interference

Figure 2-76: Advanced Settings for the Wifi Device Configuration

- **Distance Optimization (Auto-ACK Timeout)**: Determines the distance of the connected station from the AP and automatically adjusts the ACK timeout. This is disabled by default. If the stations are positioned over a wide area at different distances from the AP, it is recommended to disable this option to prevent the ACK timeout from fluctuating widely.
- **Distance (meters)**: Specifies the distance between the AP and the station, if the previous option is unchecked. Min: 300, Max: 12000 (80MHz), 24000 (40MHz), 48000 (20MHz). This value may be set to slightly more than the physical distance between the AP and the farthest station.
- **Chainmask Selection**: Sets the antenna port selection on the radio. For example, 2x2 means that 2 antennas are being used.

NOTE! The following options are for the device operating as an access point (AP).

- **Beacon Interval**: Specifies the interval between beacon transmissions by the AP, in ms. A beacon is a frame broadcast by the AP to synchronize the wireless network. For the multiple VAP case, the beacons are transmitted evenly within this interval. Thus, if four VAPs are created and the beacon interval is 200 ms, a beacon is transmitted from the radio portion every 50 ms, from each VAP in a round-robin fashion. The default value of the interval is 100 ms.

- **Adaptive noise immunity**: Controls radio sensitivity in the face of noise sources. Adaptive noise immunity allows the AP to reject spurs and non-WLAN noise. An advantage is that the AP would have to spend less time decoding the signal, resulting in lower packet loss rate.
- **Dynamic channel selection**: Automatically switches channel to avoid interference. Dynamic channel selection is feature to detect and avoid continuous wave (CW) interference. CW interference or spurs cause the noise floor to be high. This stops transmissions as well as causes receives to fail frequently. The noise floor is monitored by the calibration logic. When the noise floor is above a threshold, the AP is performs an automatic channel selection. It would disconnect from the stations (it would already have due to the interference) and move to a new channel. The stations are expected to re-associate with the AP on their own.

2.4.5.2 Interface Configuration

The Interface Configuration section contains the section tabs for:

- General Setup
- Wireless Security
- MAC-Filter
- Advanced Settings.

2.4.5.2.1 General Setup

Figure 2-77: Interface Configuration - General Setup

- **Mode**: Selects whether the device is operating as:
  - » Access Point
  - » Access Point (WDS)
  - » Station
  - » Station WDS.

NOTE! Setting more than 1 station on a board is not supported because there can only be one default gateway. This is true even if a board has both an onboard radio and a card radio. Both radios cannot be in Station mode at the same time.

- **ESSID**: Specifies the name or extended service set identifier (ESSID) of the wireless network as it is provided in the beacon message. The network name can be up to 32 characters in length and can contain spaces. When running in AP mode, it is the name of the network as advertised in the beacon message. In Station mode, it is the network name that the station associates with.
- **BSSID**: Sets the MAC address of the AP. This option is available for a device operating as a station. This is useful because there can be multiple APs with the same ESSID. Setting the MAC address would prevent the station from roaming to other APs.
- **Guard Interval**: Chooses between **Short** and **Long** guard intervals. Guard intervals are used to ensure that distinct transmissions do not interfere with one another. Data rate is improved in downlink and uplink if both AP and station use the Short Guard Interval.
- **Data Rate (Mbps)**: Selects the data rate or the modulation and coding scheme (MCS). The default setting of **Auto** is recommended. The MCS and data rates are adjusted automatically depending on the wireless channel conditions.
  - » 6 / 9 / 12 / 18 / 24 / 36 / 48 / 54 Mbps
  - » MCS 0 (13.5 Mbps) / MCS 1 (27 Mbps) / MCS 2 (40.5 Mbps) / MCS 3 (54 Mbps) / MCS 4 (81 Mbps) / MCS 5 (108 Mbps) / MCS 6 (121.5 Mbps) / MCS 7 (150 Mbps) / MCS 8 (27 Mbps) / MCS 9 (54 Mbps) / MCS 10 (81 Mbps) / MCS 11 (108 Mbps) / MCS 12 (162 Mbps) / MCS 13 (216 Mbps) / MCS 14 (243 Mbps) / MCS 15 (300 Mbps)
- **Hide ESSID**: Hides the network name (ESSID) from being broadcast publicly. (This option is for a device operating as an AP.)

NOTE!

If the goal is securing your network, use WPA or preferably WPA2 encryption. Hiding the ESSID does not provide complete security.

2.4.5.2.2 WDS

A Wireless Distribution System (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11ac network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them. The notable advantage of WDS over other solutions is it preserves the MAC addresses of client frames across links between access points.

WDS may also be considered a repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging). However, with this method, throughput is halved for all clients connected wirelessly.

2.4.5.2.3 Setup for the WDS Modes

The wireless distribution system (WDS) allows the Station WDS to bridge wireless traffic transparently, providing the functionality of a repeater. The Station WDS is a transparent client and would need to associate with an AP WDS. The WDS protocol is not defined as a standard so there may be compatibility issues between devices from different vendors. The following figures show an example of a setup.

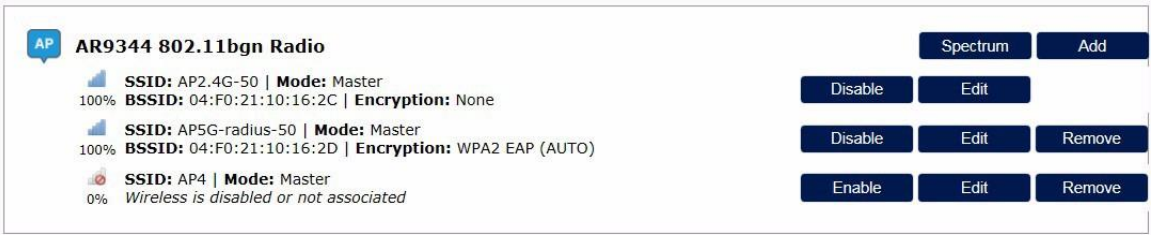

Figure 2-78: First Radio

Figure 2-79: Second Radio

Multiple stations or Stations WDS can connect to an AP WDS. In Figure 2-79, the **Add** button creates a virtual access point (VAP) on the second AP. You should choose AP WDS mode for the VAP's wireless network, e.g., "M8" so that devices in Station WDS mode can connect to this network. The pair of Station WDS and AP WDS on the same board extends the wireless coverage. If the board has two radios, one onboard and one card radio, one radio can be the Station WDS and the other radio can be the AP WDS. Therefore the Station WDS with AP WDS on the same board functions as a repeater.

In the non-WDS mode, the Station translates all the packets that pass through it to its own MAC address, thus resulting in a lack of transparency. A consequence is that the ARP table of the access point would show the MAC address of the Station assigned to IP addresses of both the Station and the computer connected to it.

2.4.5.2.4 Wireless Security

Figure 2-80: Wifi - Wireless Security

- **Encryption**: Chooses between the following encryptions:
  - » No Encryption (open)
  - » WEP Open System
  - » WEP Shared Key
  - » WPA-PSK
  - » WPA2-PSK
  - » WPA-PSK/WPA2-PSK Mixed Mode
  - » IEEE802.1X/WPA-EAP
  - » IEEE802.1X/WPA2-EAP.

2.4.5.2.4.1 WEP

Wired Equivalent Privacy (WEP) is the oldest and least secure encryption algorithm. Stronger encryption using WPA or WPA2 should be used where possible.

For the WEP Open System and WEP Shared Key encryptions, you can specify up to 4 keys and only 1 would be used at a time. We have the following options:

- **Used Key Slot**: Chooses between Key #1 to Key #4.
- **Key #1**: Specifies a string of characters to be used as the password. It may consist of 5 ASCII characters or 10 HEX characters, implying a 64-bit WEP key length. Otherwise, it may consist of 13 ASCII or 26 HEX characters, implying a 128-bit key length.
- **Key #2**, **Key #3**, and **Key #4**: Similar to Key #1.

NOTE!

Valid HEX characters are numbers 0-9 and letters A-F, case insensitive. Valid ASCII characters are numbers and the letters of the English alphabet, case sensitive. Based on the number of characters, the key is automatically checked for validity. Invalid keys are represented by red dots while valid keys are represented by black dots. Click the green arrows icon beside the text field to reveal/hide the password.

2.4.5.2.4.2 WPA or WPA2 with PSK

Wifi protected access (WPA) is a stronger encryption than WEP.

Furthermore, WPA2 was developed to strengthen the security of WPA and is stronger than WPA and WEP.

For WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK Mixed Mode encryptions, we have the following options.

- **Cipher**: Can be set to Auto, CCMP (AES), or TKIP and CCMP (AES). The Temporal Key Integrity Protocol (TKIP) was developed as a temporary replacement for WEP. The Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) is based on the Advanced Encryption Standard (AES) and is the most secure protocol.
- **Key**: The pre-shared key (PSK) is the password for the wireless network. This may consist of 8 to 63 ASCII characters.

2.4.5.2.4.3 WPA or WPA2 with EAP

The Extensible Authentication Protocol (EAP) is encapsulated by the IEEE 802.1X authentication method. IEEE 802.1X is equivalent to EAP over LAN or WLAN. Enterprise networks commonly use this authentication method.

2.4.5.2.4.4 WPA or WPA2 with EAP (AP Mode)

Figure 2-81: Encryption Options for WPA-EAP or WPA2-EAP in AP Mode

- **Cipher**: Can be set to the following:
  - » Auto
  - » CCMP (AES)
  - » TKIP and CCMP (AES).
- **Radius-Authentication-Server**: Specifies the IP address of the RADIUS authentication server.

NOTE! Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service.

- **Radius-Authentication-Port**: Sets the port number for the RADIUS authentication server. Normally, the port number is 1812.
- **Radius-Authentication-Secret**: Configures the password for the authentication transaction.
- **Radius-Accounting-Server**: Specifies the IP address of the RADIUS accounting server.
- **Radius-Accounting-Port**: Sets the port number for the RADIUS accounting server. Normally, the port number is 1813.
- **Radius-Accounting-Secret**: Configures the password for the accounting transaction.
- **NAS ID**: Specifies the identity of the network access server (NAS).

2.4.5.2.4.5 WPA or WPA2 with EAP (Station Mode)

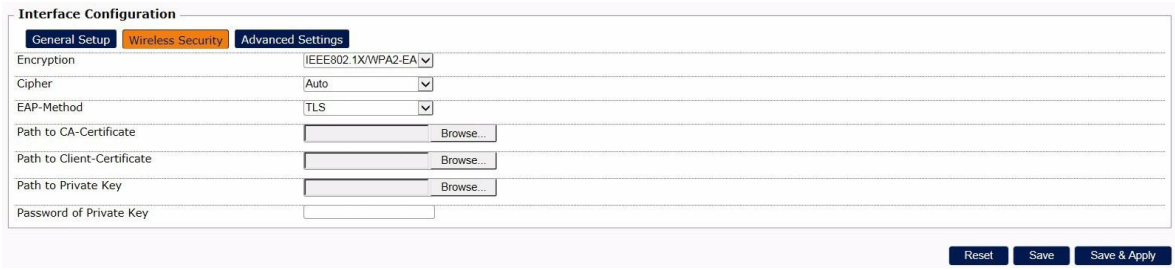

Figure 2-82: Encryption Options for WPA-EAP or WPA2-EAP in Station Mode

- **Cipher**: Can be set to the following:
  - » Auto
  - » CCMP (AES)
  - » TKIP and CCMP (AES).
- **EAP-Method**: The authentication protocol can be set to Transport Layer Security (**TLS**), Tunneled TLS (**TTLS**), or Protected EAP (**PEAP**).
- **Path to CA-Certificate**: Selects the file for the CA certificate.

NOTE! The certificate authority (CA) is a trusted third party that issues digital certificates. In a public key infrastructure scheme, a digital certificate certifies the ownership of a public key by the named subject of the certificate.

- **Path to Client-Certificate**: Selects the file for the client certificate.

Options for TLS as the EAP method

- **Path to Private Key**: Selects the file for the private key.
- **Password of Private Key**: Configures the password for the private key.

Options for TTLS or PEAP as the EAP method

- **Authentication**: Selects the authentication method used by the AP, e.g., PAP, CHAP, MSCHAP, or MSCHAPV2.
- **Identity**: Sets the identity used by the supplicant for EAP authentication.
- **Password**: Sets the password used by the supplicant for EAP authentication.

2.4.5.2.5 MAC-Filter

This section tab is only available for a device operating as an AP.

Figure 2-83: Wifi AP MAC Filter

- **MAC-Address Filter**: Lets you allow only devices with the listed MAC address to associate with this AP, or lets you block devices with the listed MAC address.
- MAC-List: Adds the MAC address of the remote device to either block or allow.

2.4.5.2.6 Advanced Settings

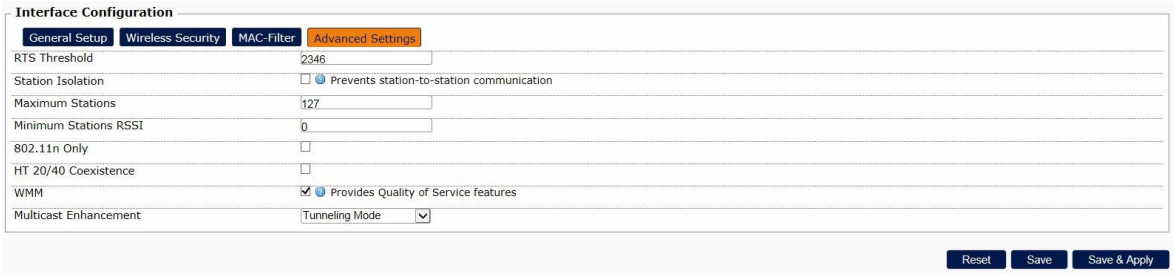

Figure 2-84: Advanced Settings for the Wifi Interface

- **RTS Threshold**: Sets the threshold for the packet size above which the request to send (RTS) mechanism is used. The default is 2346 octets. There is a trade-off to consider when setting this parameter. On the one hand, using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, and therefore reducing the throughput of the network packet. On the other hand, when more RTS packets are sent, the system recovers faster from interference or collisions. This is useful in a heavily loaded network, or a wireless network with high electromagnetic interference.

NOTE!

The following options for Station Isolation, Maximum Stations, Minimum Stations RSSI, and 802.11n Only are available only for a device operating as an AP.

- **Station Isolation**: Prevents station-to-station communication, unchecked by default. When Station Isolation is disabled, wireless clients can communicate with one another normally by sending traffic through the AP. When Station Isolation is enabled, the AP blocks communication between wireless clients on the same AP.
- **Maximum Stations**: Specifies the maximum number of associated stations, the default being 127.
- **Minimum Stations RSSI**: Sets the minimum received signal strength indicator for a station to be associated. The default value of 0 means that the AP would allow a station to associate independent of its RSSI.
- **802.11n Only**: Forces the device to use only the IEEE802.11n standard, unchecked by default.
- **HT 20/40 Coexistence**: Allows the network to use both 20 MHz and 40 MHz bands. Required on AP side primarily to support co-existence. The station can also send intolerant bit status to AP to signal use of 20 MHz channel. The station follows the AP's channel bonding and channel switching HT 20/40 mechanism. Disabling this setting forces the use of 40 MHz bandwidth/channel bonding, and results in high data rate.
- **WMM**: Provides Quality of Service (QoS) features, checked by default. Wireless multimedia enables the classification of the network traffic into 4 main types, voice, video, best effort, and background, in decreasing order of priority. Higher priority traffic has a higher transmission opportunity and would have to wait less time to transmit. As a result, an existing video stream would not be interrupted by additional background processes.
- **Multicast Enhancements**
  - » Tunneling Mode
  - » Translating Mode

2.4.6 V

A
V
d

T

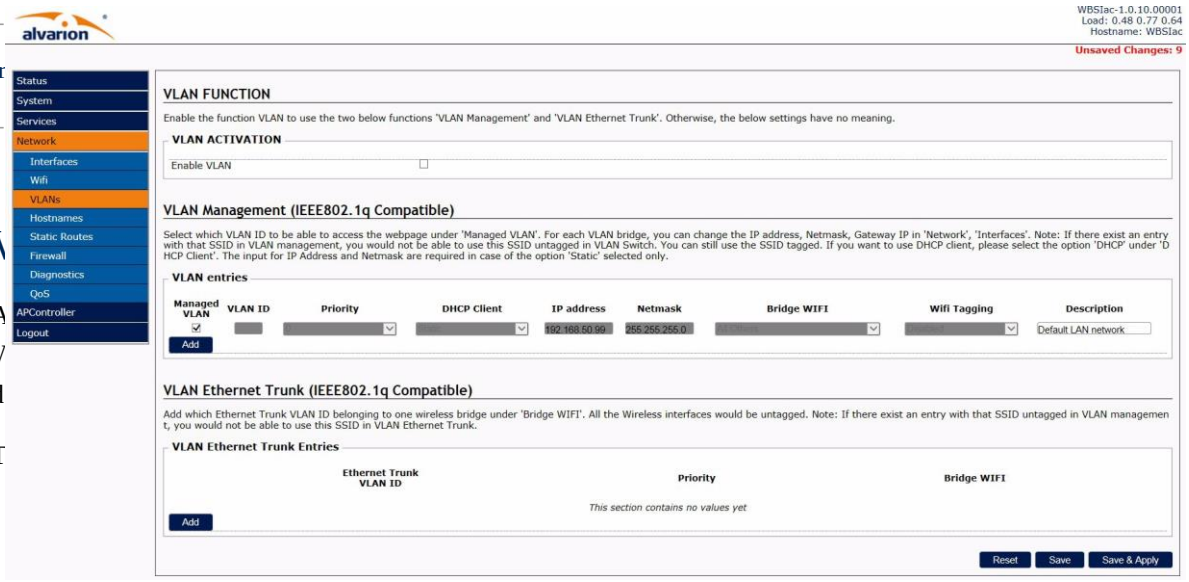
alvarion
WBSIac-1.0.10.00001
Load: 0.48 0.77 0.64
Hostname: WBSIac
Unsaved Changes: 9
Status
System
Services
Network
Interfaces
Wifi
VLANs
Hostnames
Static Routes
Firewall
Diagnostics
QoS
APController
Logout
VLAN FUNCTION
Enable the function VLAN to use the two below functions 'VLAN Management' and 'VLAN Ethernet Trunk'. Otherwise, the below settings have no meaning.
VLAN ACTIVATION
Enable VLAN
VLAN Management (IEEE802.1q Compatible)
Select which VLAN ID to be able to access the webpage under 'Managed VLAN'. For each VLAN bridge, you can change the IP address, Netmask, Gateway IP in 'Network', 'Interfaces'. Note: If there exist an entry with that SSID in VLAN management, you would not be able to use this SSID untagged in VLAN Switch. You can still use the SSID tagged. If you want to use DHCP client, please select the option 'DHCP' under 'DHCP Client'. The input for IP Address and Netmask are required in case of the option 'Static' selected only.
VLAN entries
Managed VLAN
VLAN ID
Priority
DHCP Client
IP address
Netmask
Bridge WIFI
Wifi Tagging
Description
192.168.60.99
255.255.255.0
Default LAN network
Add
VLAN Ethernet Trunk (IEEE802.1q Compatible)
Add which Ethernet Trunk VLAN ID belonging to one wireless bridge under 'Bridge WIFI'. All the Wireless interfaces would be untagged. Note: If there exist an entry with that SSID untagged in VLAN management, you would not be able to use this SSID in VLAN Ethernet Trunk.
VLAN Ethernet Trunk Entries
Ethernet Trunk VLAN ID
Priority
Bridge WIFI
This section contains no values yet
Add
Reset
Save
Save & Apply

Figure 2-85: VLAN Management

2.4.6.1 VLAN Function

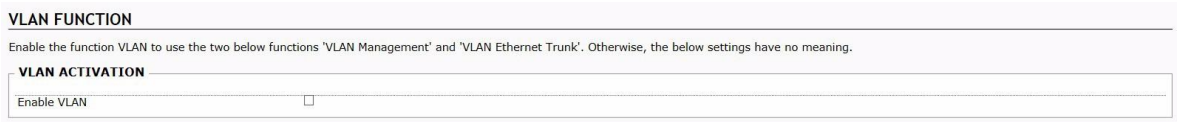
VLAN FUNCTION
Enable the function VLAN to use the two below functions 'VLAN Management' and 'VLAN Ethernet Trunk'. Otherwise, the below settings have no meaning.
VLAN ACTIVATION
Enable VLAN

Figure 2-86: VLAN Activation

- **Enable VLAN**: Activate this checkbox option to enable the "VLAN Management" and "Managed VLAN" functions. If this option is disabled, the "VLAN Management" and "Managed VLAN" functions are inactive.

2.4.6.2 VLAN Management

The VLAN Management section controls individual VLANs according to the IEEE802.1Q standards. Within the subsection for VLAN entries, each row represents one VLAN ID.

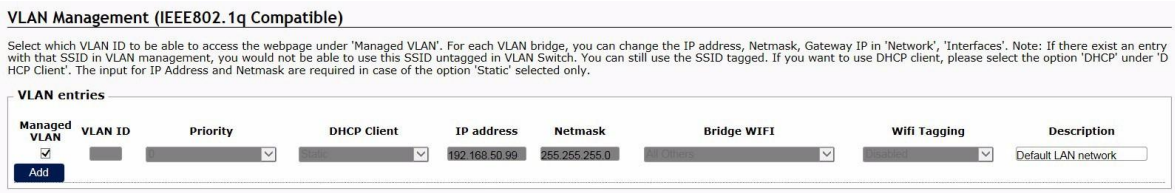
VLAN Management (IEEE802.1q Compatible)
Select which VLAN ID to be able to access the webpage under 'Managed VLAN'. For each VLAN bridge, you can change the IP address, Netmask, Gateway IP in 'Network', 'Interfaces'. Note: If there exist an entry with that SSID in VLAN management, you would not be able to use this SSID untagged in VLAN Switch. You can still use the SSID tagged. If you want to use DHCP client, please select the option 'DHCP' under 'DHCP Client'. The input for IP Address and Netmask are required in case of the option 'Static' selected only.
VLAN entries
Managed VLAN
VLAN ID
Priority
DHCP Client
IP address
Netmask
Bridge WIFI
Wifi Tagging
Description
192.168.50.99
255.255.255.0
Default LAN network
Add

Figure 2-87: VLAN Entries in the VLAN Management Section

The first row is given by default. It is the native or untagged VLAN.

- **Add**: Inserts a new row corresponding to a new VLAN. The IP address field should be distinct for different devices.
- **Managed VLAN**: Allows computers on this VLAN to access the device's configuration web page.
- **VLAN ID**: Specifies the identifier for the VLAN. It is an integer from 2 to 4094. Let VID be this number. The "eth0" port is tagged with VID to give "eth0.VID". This port can have multiple tags corresponding to different VLANs. An "eth0.VID" port would only accept frames that have been tagged with the VLAN ID VID.
- **Priority**: Chooses the priority for transmitting packets. This is a number from 0 to 7. The number 7 represents the highest priority.
- **DHCP Client**: Displays the DHCP client
- **IP address**: Sets the IP address of the AP as seen by other devices on this VLAN.
- **Netmask**: States the netmask of the subnet defined by this VLAN.
- **Bridge WIFI**: Selects the wireless network for which its interface would be bridged to the "eth0.VID" port. The choice All Others would select all other wireless networks that are currently not selected.
- **Wifi Tagging**: Should be set to Enabled. This tags the Ethernet frames sent over Wifi. This does not add a second tag (QinQ). The wireless interface "ath0" of this VLAN would be tagged to give "ath0.VID" for example.
- **Description**: Provides a short description of the VLAN.

2.4.6.3 VLAN Ethernet Trunk

The VLAN Ethernet Trunk uses a wireless network as a trunk link to connect physically separate VLANs having the same VLAN ID.

Within the subsection for the VLAN Ethernet Trunk Entries, each row represents one VLAN ID.

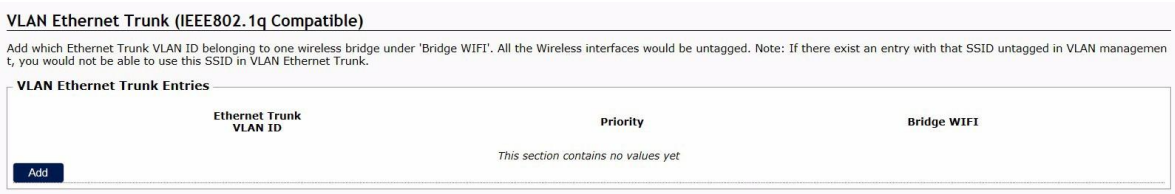
VLAN Ethernet Trunk (IEEE802.1q Compatible)
Add which Ethernet Trunk VLAN ID belonging to one wireless bridge under 'Bridge WIFI'. All the Wireless interfaces would be untagged. Note: If there exist an entry with that SSID untagged in VLAN managemen t, you would not be able to use this SSID in VLAN Ethernet Trunk.
VLAN Ethernet Trunk Entries
Ethernet Trunk VLAN ID
Priority
Bridge WIFI
This section contains no values yet
Add

Figure 2-88: VLAN Entries in the VLAN Ethernet Trunk Section

- **Add**: Inserts a new row corresponding to a new VLAN. The IP address field should be distinct for different devices.
- **Ethernet Trunk VLAN ID**: Sets the VLAN ID of the separate VLANs to connect.
- **Priority**: Chooses the priority for transmitting packets. This is a number from 0 to 7. The number 7 represents the highest priority.
- **Bridge WIFI**: Selects the wireless network that would act as a trunk link.

2.4.7 Hostnames

In the **Network > Hostnames** page, you can specify custom hostnames (URLs) with their respective IP addresses. This is an additional local DNS.

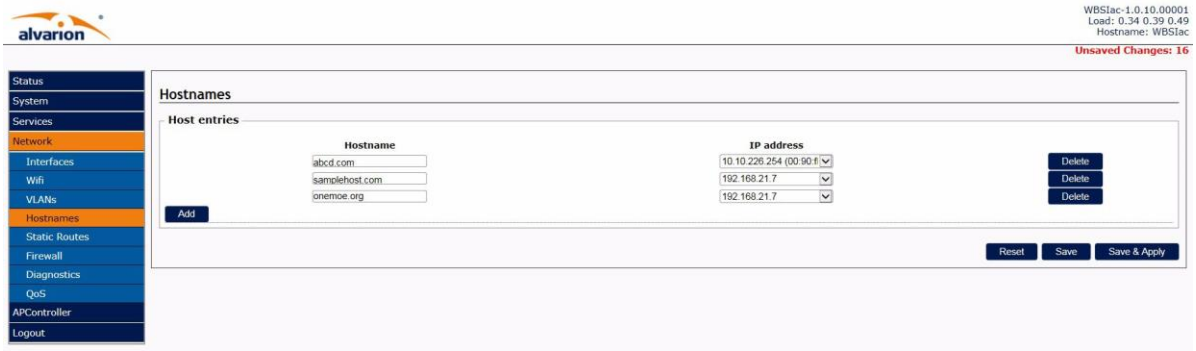

Figure 2-89: Custom Hostname Entries

NOTE!

The computers in the same subnet need to set the IP address of this device as their preferred DNS server in order to interpret these custom hostnames.

2.4.8 Static Routes

The **Network > Static Routes** page shows the static IPv4 routes.

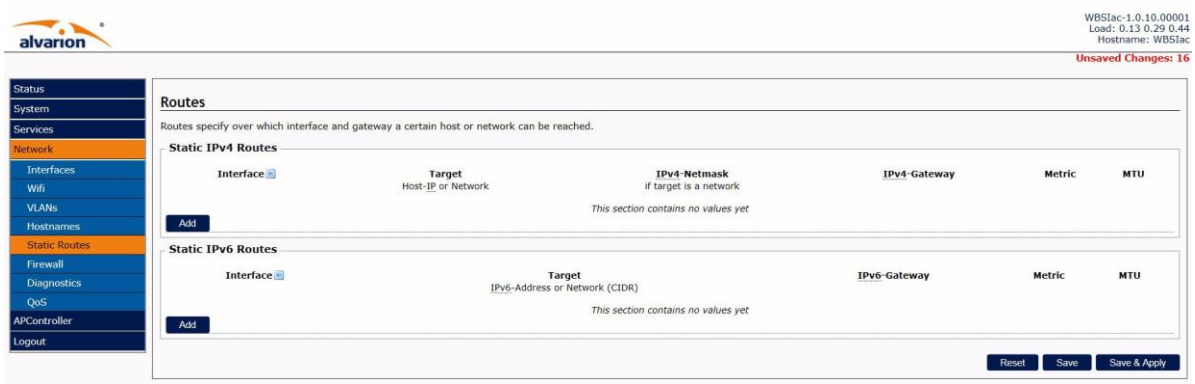

Figure 2-90: Static IPv4 and IPv6 Routes

Each row shows the interface and gateway over which a certain host or network can be reached.

2.4.9 Firewall

The **Network > Firewall** page consists of the following tabs:

- General Settings
- Port Forwards
- Traffic Rules.

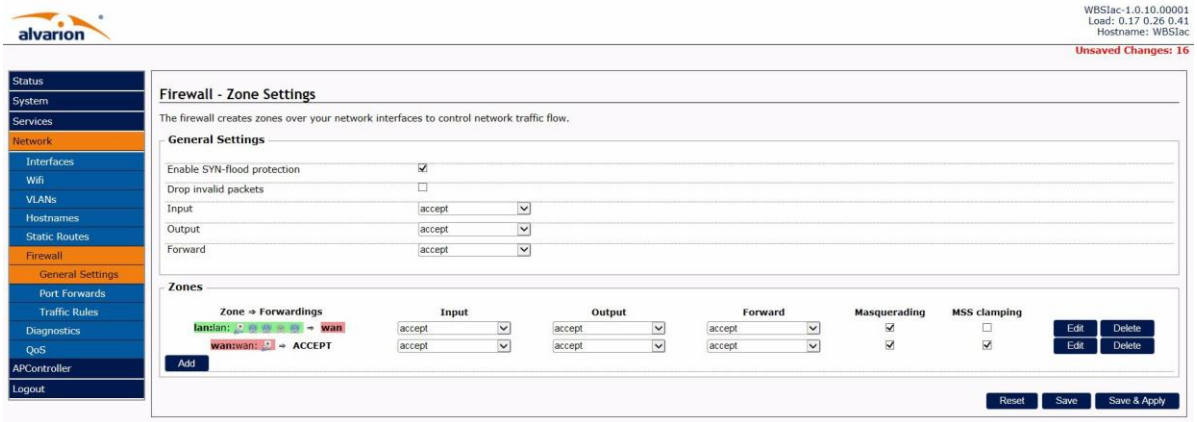

Figure 2-91: Firewall Page

2.4.9.1 General Settings

The firewall creates zones over the network interfaces to control network traffic flow.

The **Network > Firewall > General Settings** page contains the zone settings.

Figure 2-92: Firewall - General Settings

- **Enable SYN-flood protection**: Checked by default.
- **Drop invalid packets**: Unchecked by default.
- **Input**: To accept by default.
- **Output**: To accept by default.
- **Forward**: To reject by default.

2.4.9.1.1 Zones

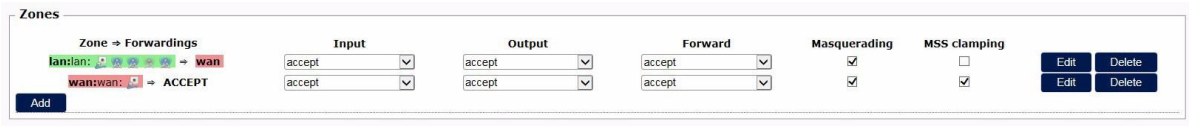

Figure 2-93: Default Settings for the Firewall Zones

- Zone > Forwardings
- Input
- Output
- Forward
- Masquerading
- MSS Clamping
- Edit
- Delete
- Add

2.4.9.1.1.1 Editing a Zone

Clicking the **Edit** button allows you to edit the **Firewall - Zone Settings**.

This section defines common "lan" properties. The input and output options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for forwarded traffic between different networks within the zone. Covered networks specifies which available networks are member of this zone.

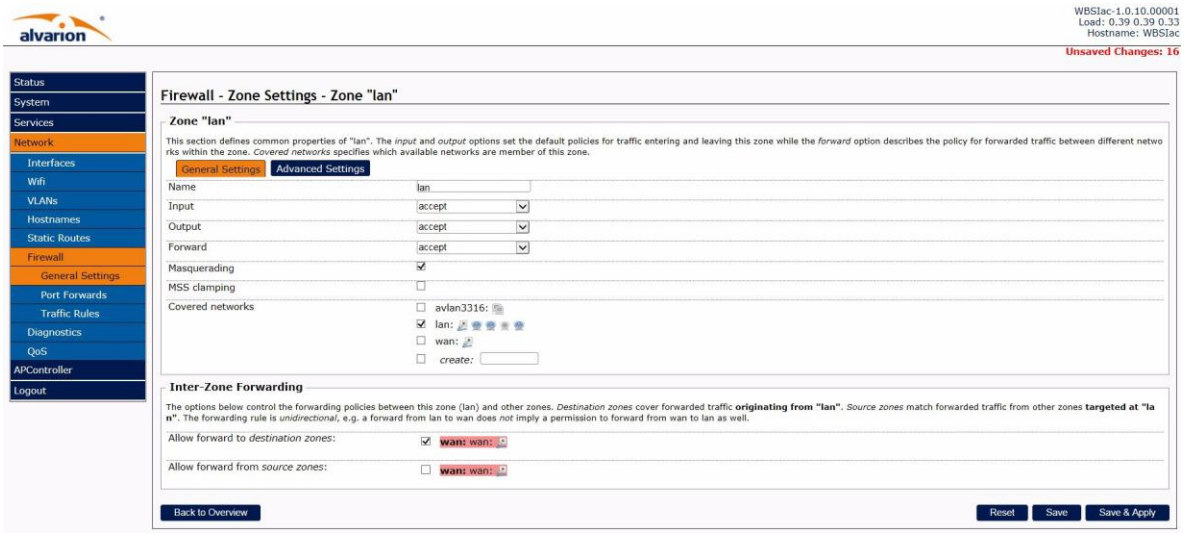

Figure 2-94: Editing the Firewall - Zone Settings

- **Zone "lan" General Settings** tab: Allows you to edit the following Firewall - Zone Settings "lan" parameters:
  - Name
  - Input
  - Output
  - Forward
  - Masquerading
  - MSS clamping
  - Covered networks

- **Zone "lan" Advanced Settings** tab: Allows you to edit the following Firewall - Zone Settings advanced "lan" parameters:
  - » Restrict to address family
    - IPv4 and IPv6
    - IPv4 only
    - IPv6 only
  - » Restrict Masquerading to given source subnets
  - » Restrict Masquerading to given destination subnets
  - » Force connection tracking
  - » Enable logging on this zone
- Inter-Zone Forwarding section

  The lnter-Zone Forwarding options control the forwarding policies between this zone (lan) and other zones. Destination zones cover forwarded traffic originating from "lan". Source zones match forwarded traffic from other zones targeted at "lan". The forwarding rule is unidirectional, e.g., a forward from lan to wan does not imply a permission to forward from wan to lan as well.
  - » Allow forward to destination zones
  - » Allow forward to source zones

2.4.9.1.1.2 Adding a Zone

Clicking the Add button allows you to add a zone in the Firewall.

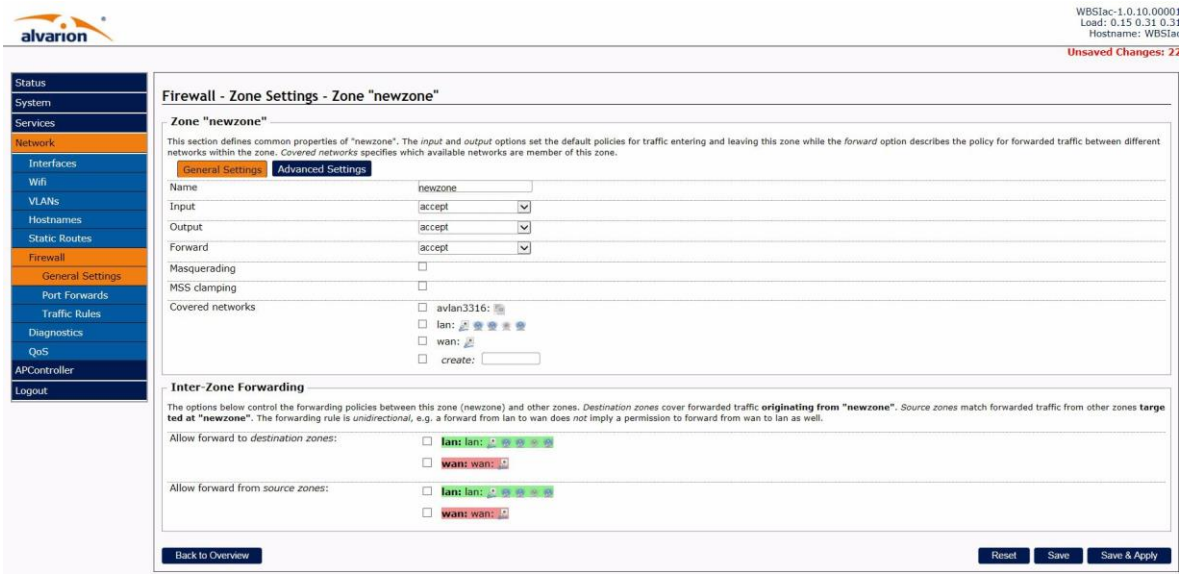

Figure 2-95: Adding a Zone

The parameters are the same as when you are editing a zone, only in this case you might have to provide the appropriate values for a new zone. For more details on the parameters when defining a new zone, see Section 2.4.9.1.1.1 Editing a Zone.

2.4.9.2 Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

The **Network > Firewall > Port Forwards** page lets you define the protocol and port number to access an internal IP address.

Figure 2-96: Adding a Port Forwarding Rule

2.4.9.2.1 Editing Fort Forwards

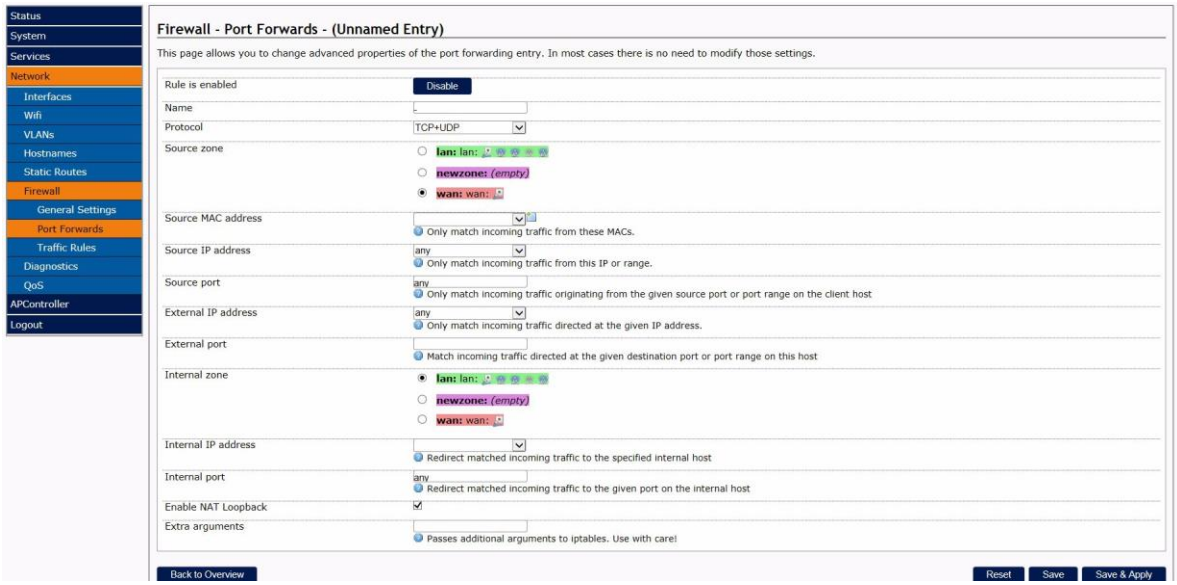

Figure 2-97: Editing Firewall - Port Forwards

The **Firewall - Port Forwards** page allows you to change advanced properties of the port forwarding entry. In most cases there is no need to modify the settings.

The following are the Firewall - Port Forwards parameters that can be edited:

- **Rule is enabled**: Enabled by default
- **Name**: The name of the port forwarding entry
- **Protocol**: Select from the following protocols: TCP+UDP, TCP, UDP, ICMP or custom
- **Source zone**: Select the source zone: WAN, LAN or a new zone
- **Source MAC address**: Select a MAC address that only matches incoming traffic from these MACs.
- **Source IP address**: Select an IP address that only matches incoming traffic from the IP or range; default is "any".
- **Source Port**: Select a source port that only matches incoming traffic originating from the given source port or port range on the client host; default is "any".
- **External IP address**: Select an external IP address that only matches incoming traffic directed at the given IP address; default is "any".
- **External Port**: Matches the incoming traffic directed at the given destination port or port range on the host.
- **Internal Zone**: Select an internal zone, i.e., LAN, WAN or a new zone
- **Internal IP address**: The IP address where to redirect matched incoming traffic to the specified internal host
- **Enable NAT loopback**: Enabled by default
- **Extra arguments**: Passes additional arguments to iptables.

2.4.9.3 Traffic Rules

The **Network > Firewall > Traffic Rules** page configures the traffic rules and source NAT.

2.4.9.3.1 Traffic Rules

Traffic rules define policies for packets travelling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the AP.

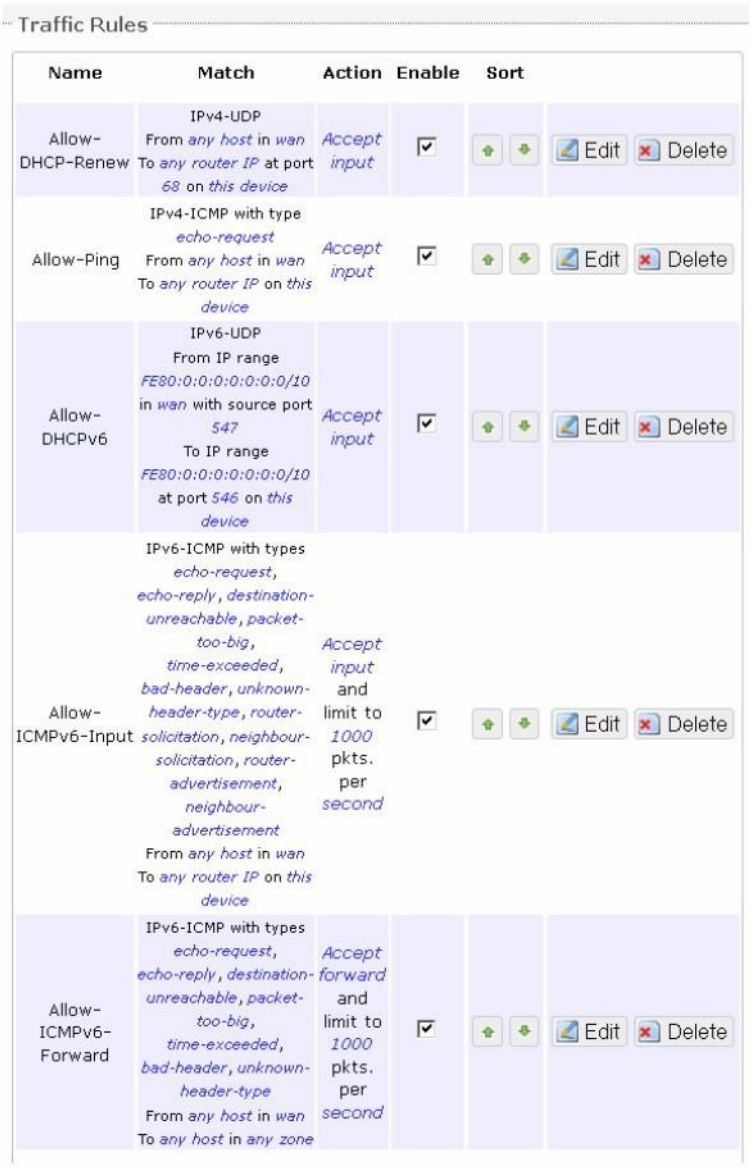
Traffic Rules
Name
Match
Action
Enable
Sort
Allow-DHCP-Renew
IPv4-UDP From any host in wan To any router IP at port 68 on this device
Accept input
Edit
Delete
Allow-Ping
IPv4-ICMP with type echo-request From any host in wan To any router IP on this device
Accept input
Edit
Delete
Allow-DHCPv6
IPv6-UDP From IP range FE80:0:0:0:0:0:0:0/10 in wan with source port 547 To IP range FE80:0:0:0:0:0:0:0/10 at port 546 on this device
Accept input
Edit
Delete
Allow-ICMPv6-Input
IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement From any host in wan To any router IP on this device
Accept input and limit to 1000 pkts. per second
Edit
Delete
Allow-ICMPv6-Forward
IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type From any host in wan To any host in any zone
Accept forward and limit to 1000 pkts. per second
Edit
Delete

Figure 2-98: Firewall Traffic Rules (Default Settings)

Figure 2-99: Firewall Traffic Rules - Lower Part

2.4.9.3.2 Source NAT

So
fo

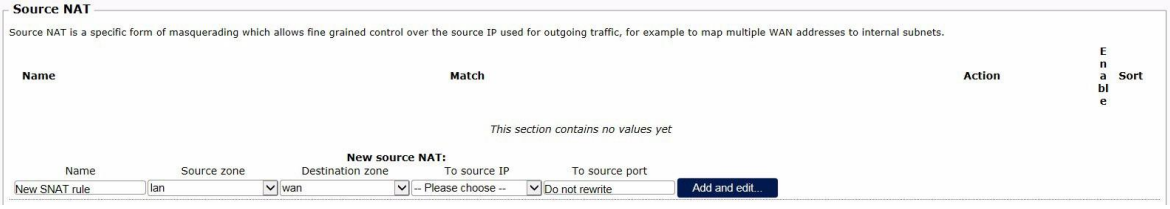

Figure 2-100: Source NAT

2.4.10 Diagnostics

2.4.10.1 Network Utilities

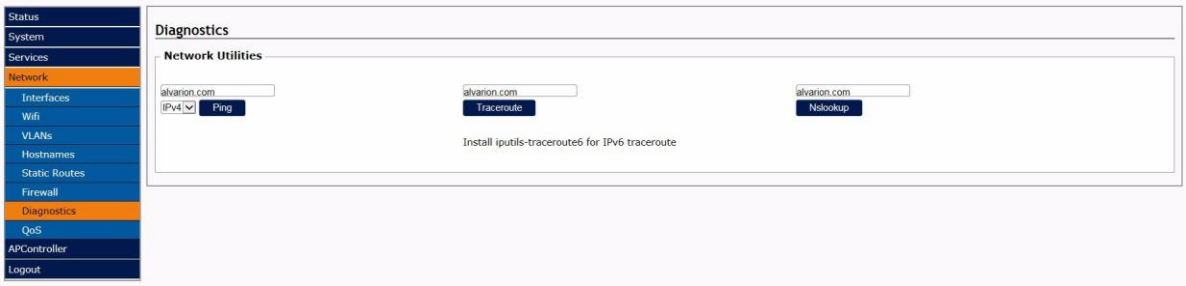

Figure 2-101: Network Utilities

Network Utilities consists of the following:

- Ping
- Traceroute
- Nslookup

2.4.10.1.1 Ping

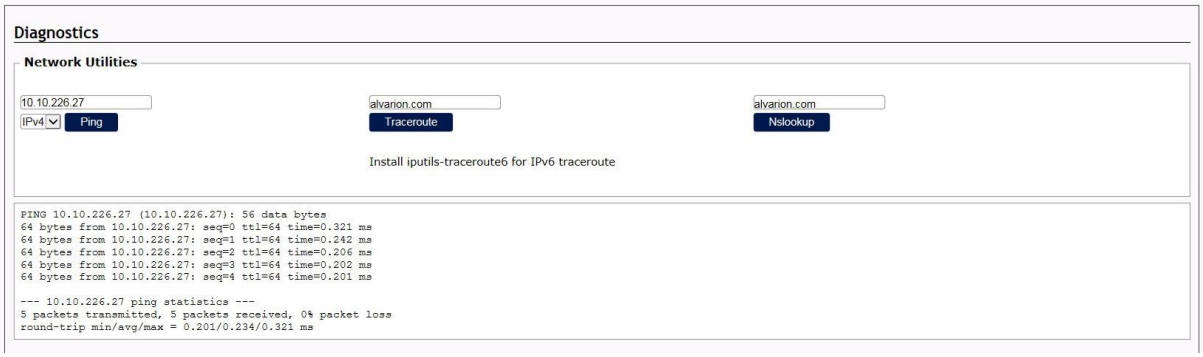
Diagnostics
Network Utilities
10.10.226.27
IPv4
Ping
alvarion.com
Traceroute
alvarion.com
Nslookup
Install iputils-traceroute6 for IPv6 traceroute
PING 10.10.226.27 (10.10.226.27): 56 data bytes
64 bytes from 10.10.226.27: seq=0 ttl=64 time=0.321 ms
64 bytes from 10.10.226.27: seq=1 ttl=64 time=0.242 ms
64 bytes from 10.10.226.27: seq=2 ttl=64 time=0.206 ms
64 bytes from 10.10.226.27: seq=3 ttl=64 time=0.202 ms
64 bytes from 10.10.226.27: seq=4 ttl=64 time=0.201 ms
--- 10.10.226.27 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.201/0.234/0.321 ms

Figure 2-102: Result of Ping

2.4.10.1.2 Traceroute

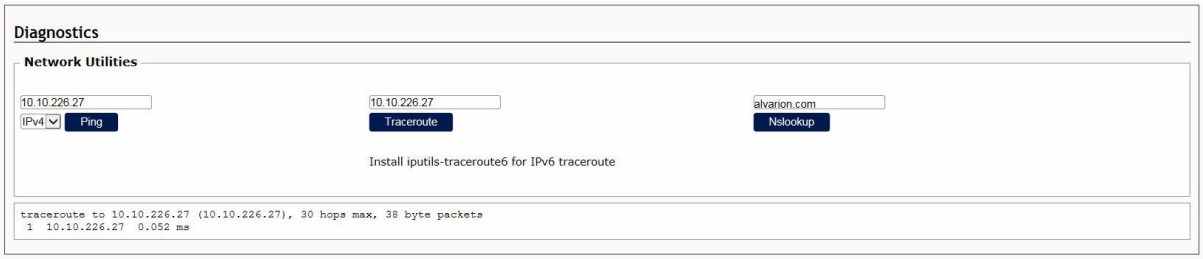

Figure 2-103: Result of Traceroute

2.4.10.1.3 Nslookup

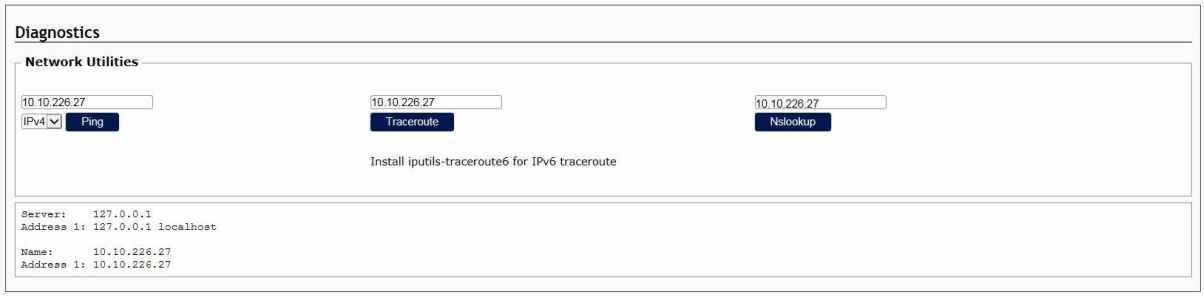

Figure 2-104: Result of Nslookup

2.4.11 Quality of Service

The **Network > QoS** page configures the quality of service (QoS). With QoS, you can prioritize network traffic selected by addresses, ports, or services. You can limit the download and upload speeds. Network QoS is disabled by default.

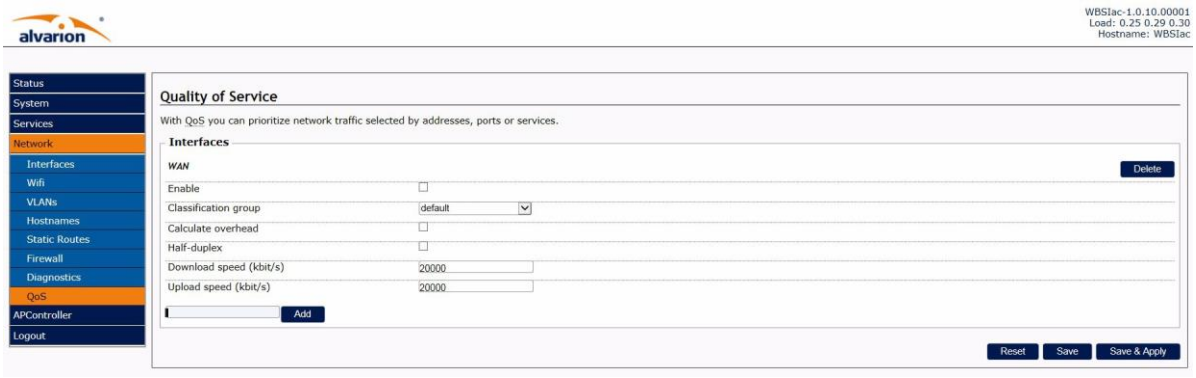

Figure 2-105: Network QoS Settings

- **Enable**: Click to enable this QoS option
- **Classification group**
- **Calculate overhead**: Click to enable calculating the overhead option
- **Half-duplex**: Disabled by default
- **Download speed (kbit/s)**: Default is 20000 kbit/s
- **Upload speed (kbit/s)**: Default is 20000 kbit/s

2.5 Arena Controller Tab

APs running the WBSIac AP firmware can be managed by the Arena Controller.

The Arena Controller sends and receives information from the WBSIac APs using the SNMP protocol.

The settings can be seen by clicking the Arena controller top-level tab.

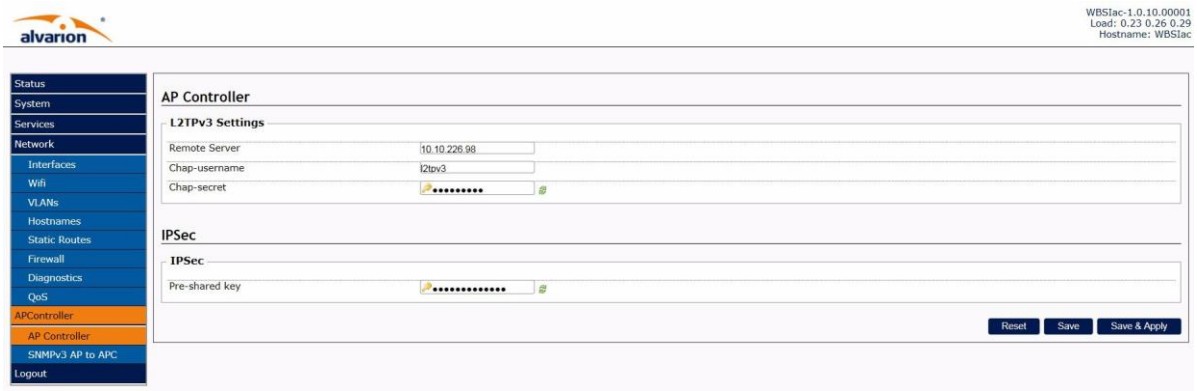

Figure 2-106: Arena Controller Tab

When using the Arena Controller for the first time, you only need to set the IP address of the Arena Controller. This has to be done in the AP's configuration web page itself. All other settings should remain as the default values for now.

Always click **Save & Apply**. Do not just click **Save**. This is to apply the settings immediately.

2.5.1 L2TPv3 Settings

Figure 2-107: L2TPv3 Settings

The following are the settings for the Layer 2 Tunneling Protocol Version 3 (L2TPv3).

- **Remote Server**: Configures the IP address of the Arena Controller, e.g., 192.168.3.178.
- **Chap-username**: Sets the username for the Challenge-Handshake Authentication Protocol (CHAP).
- **Chap-secret**: Sets the password for the Challenge-Handshake Authentication Protocol (CHAP).

2.5.2 IPSec

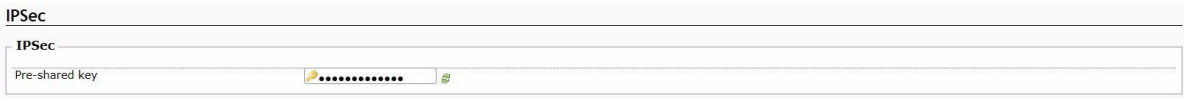

Figure 2-108: IPSec

By default, the Internet Protocol Security (IPsec) is disabled for the WBSIac boards to decrease the usage of the CPU resources. It can also be enabled.

The L2TPv3 itself already provides data channel protection against malicious data insertion.

- **Pre-shared key**: Sets the password for the IPsec.

2.5.3 Arena Controller SNMP Settings

The **SNMPv3 AP to ARENA CONTROLLER** section contains the Arena Controller SNMP settings.

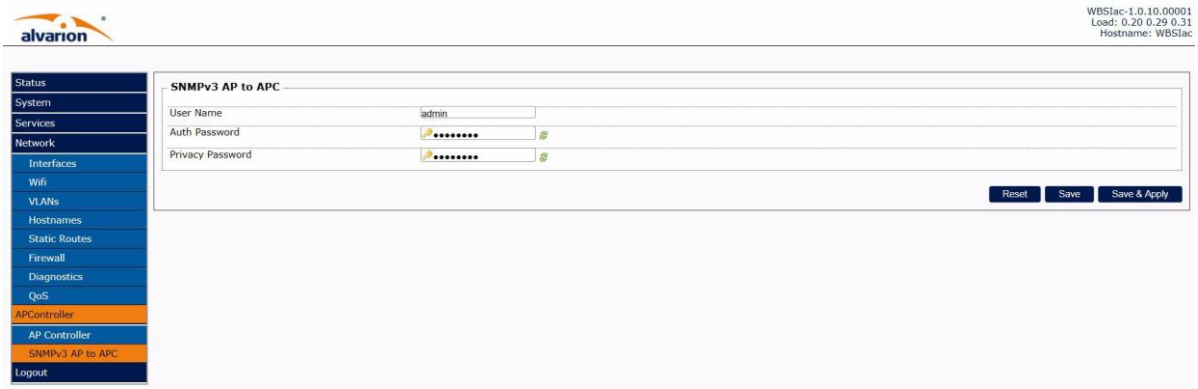

Figure 2-109: SNMPv3 AP to ARENA CONTROLLER

Currently, the following default values must be used.

- User Name: "admin"
- Auth Password: "password"
- Auth Password: "password"

2.5.4 A

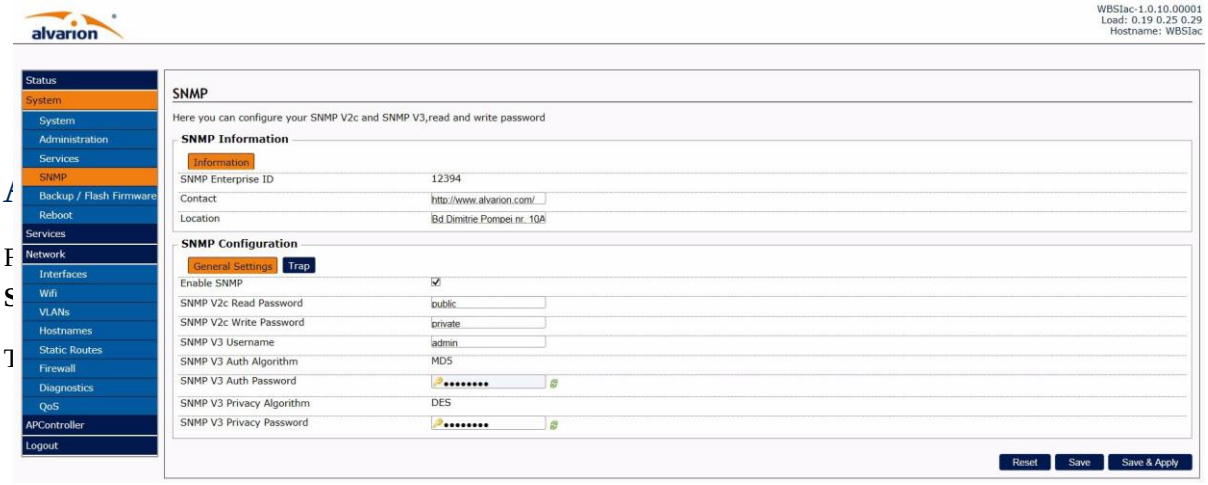

Figure 2-110: AP SNMP Settings

2.6 Logout

Click the **Logout** tab to exit the WBSIac AP application.

Chapter 3 - Final Notes

In this Chapter:

- Troubleshooting

3.1 Troubleshooting

3.1.1 The PC Cannot Connect to the WBSIac AP

The configuration web page for the WBSIac AP would not be able to show up if the WBSIac AP and your computer are not connected.

If the PC and the WBSlac AP are joined to the network by LAN cables, they would not be able to connect if any of the network cable connections are loose. A possible indicator is that there is no light at the LAN port of the PC. In Windows, if you click the network icon and click **View network connections**, the LAN port shows **Disconnected**. Ensure that all the connections are tight.

Sometimes, disconnecting and reconnecting the LAN cable solves connection problems if DHCP is used, because the DHCP server and DNS server are reset.

The WBSIac AP, the computer, and the gateway must have IP addresses on the same network. For example, if you use a subnet mask of 255.255.255.0 and the gateway IP address is 192.168.3.1, all the IP addresses must be unique and be of the form 192.168.3.X.

Check whether the WBSIac AP and your computer are connected on the same network by running the ping command to ping the IP address of the WBSIac AP. Alternatively, type the following in the AP's Linux terminal:

```
ping 192.168.3.77
```

if your computer's IP address is 192.168.3.77 for example.

There should be ping responses.

An IP address conflict would cause unstable pings. Switch to another address and ping the conflicting address to check.

If using a Windows computer, you should run the command **arp -d *** if the network configuration has changed. This is to delete the address resolution protocol (ARP) table in Windows as it may not update fast enough.

If the ping still cannot get responses, try disabling the firewall on your Windows computer. The Windows Firewall on your computer may prevent it from sending back a ping response. Disabling the firewall may be a security risk, so you should take the precaution of disconnecting the Internet first.

3.1.2 PC Ethernet and Wifi Adapters

If your PC has both Ethernet and Wifi adapters, they must not have the same subnet. Otherwise, packets from the PC may not be directed to the correct network.

3.1.3 The Mobile Phone Cannot Connect

A mobile phone or any Wifi user would not be able to connect to a wireless AP if a DHCP server on the network does not exist. Ensure that there is one, and only one, DHCP server to assign IP addresses automatically to users.

You may refer to Section 2.4.3.2 DHCP Server to enable the DHCP server for an AP.

3.1.4 The Mobile Phone Connects but cannot Access the Internet

A mobile phone or any connected Wifi user would not be able to access the Internet if the default gateway is not set correctly on the WBSIac AP.

If the WBSIac AP has enabled a DHCP server but the gateway is at a different IP address, add a DHCP option according to Section 2.4.3.2 DHCP Server.

The DNS server should also be set.

3.1.5 Unresponsive Web Page

Symptom:

The **XML Parsing Error** may occur if a certain option was changed and the web page did not update in time.

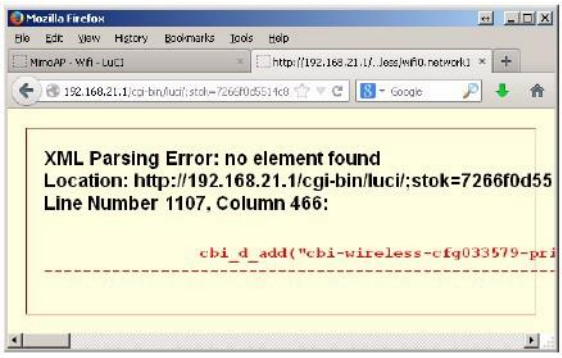

Figure 3-1: XML Parsing Error

Solution:

Re-enter the IP address into the browser. For example, if the current URL is 192.168.21.1/cgi-bin/luci/;stok=7266f0d55..., delete the right hand side to leave the IP address of 192.168.21.1 and press **Enter**. This would bring you back to the login page of the device.

3.1.6 Unresponsive AP

Symptom:

The WBSIac AP does not respond.

Solution:

Turn off the WBSIac AP for 10 seconds and then turn it on again.

3.2 Resetting to Factory Default

To reset the WBSIac AP to factory default settings while the power is on, hold down the reset button for 8 seconds and then release.

Another method is to enter the following command into the WBSIac AP's Linux terminal:

```
mtd -r erase rootfs_data
```

After a while, the flash would be erased and the WBSIac AP would reboot into its factory default state. The firmware version remains the same as the latest firmware loaded onto the board.

Glossary

AP	Access Point
	A device that provides network access to associated stations (connected wireless devices). A wireless router can function as an AP.
ACK	Acknowledgment
	This is a response to a transmission to indicate that the data packet was received correctly.
ARP	Address Resolution Protocol
	This is a broadcast protocol for mapping IP addresses to MAC addresses.
CHAP	Challenge-Handshake Authentication Protocol
	This is a protocol for authenticating users to an ISP.
CPE	Customer-Premises Equipment
	This is also known as a station.
dB	Decibels
	This is a measure of intensity.
dBm	Decibel-milliwatts
	This is a measure of power relative to 1 mW. It is commonly used to measure wireless signal power. A higher power leads to better signal quality.
DDNS	Dynamic DNS
	This is a system for updating domain names in real time. It allows a domain name to be assigned to a device with a dynamic IP address.

DHCP Dynamic Host Configuration Protocol

This is a protocol for allocating IP addresses dynamically so that addresses can be reused when hosts (e.g., computers) no longer need them.

DNS Domain Name System

This is a distributed and hierarchical naming system for computers, services, or any resource connected to the Internet or a private network.

EIRP Equivalent Isotropically Radiated Power

Each country sets the legally permitted maximum for the EIRP limits on each channel.

ESSID Extended Service Set Identifier

This is the name of the wireless network. It is case-sensitive and up to 32 alphanumeric characters in length. The ESSID differentiates one wireless network from another. All access points and devices trying to connect to a specific wireless network should use the same ESSID (and password) to enable effective roaming.

FTP File Transfer Protocol

This is a protocol for transferring files between network nodes.

HTTP Hypertext Transfer Protocol

This is a protocol used by web browsers and web servers to transfer files.

IP Internet Protocol

This is the primary communications protocol used for relaying network packets (also known as datagrams) across an internetwork using the Internet Protocol Suite. IP is responsible for routing packets across network boundaries. It is the principle protocol that establishes the Internet.

ISP Internet Service Provider

L2TP Layer 2 Tunneling Protocol

This is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

LAN Local Area Network

Layer 2 Data link layer of the Open Systems Interconnection (OSI) model

This corresponds to the Link layer of the Internet protocol suite.

MAC Address Media Access Control Address

This is a globally unique identifier attached to a network adapter. It also identifies the hardware manufacturer.

Mbps	Megabits per second Also Mbit/s. This is a measure of the data rate.
MiniPCIe	Mini Peripheral Component Interconnect Express A miniPCIe radio is a radio card that can be inserted into a AP's circuit board.
MTU	Maximum Transmission Unit This is the size, in bytes, of the largest packet that can be passed on. The MTU for Ethernet is a 1500-byte packet.
NAT	Network Address Translation This is the process of rewriting IP addresses as a packet passes through a controller or firewall. NAT enables multiple computers (or hosts) on a LAN to access the Internet using the single public IP address of the LAN's gateway controller.
NMS	Network Management Station This is a software which runs on the SNMP manager. It is sometimes simply referred to as an SNMP manager.
NTP	Network Time Protocol This is a protocol for synchronizing a controller to a single clock on the network, known as the clock master.
PAP	Password Authentication Protocol This is a protocol for authenticating users to a remote access server or ISP.
PPPoE	Point-to-Point Protocol over Ethernet This is a protocol for connecting a network of hosts to an ISP without the ISP having to manage the allocation of IP addresses.
PPTP	Point-to-Point Tunneling Protocol This is a protocol for the creation of VPNs for the secure transfer of data from remote clients to private servers over the Internet.
QoS	Quality of Service This is the prioritization of network traffic. Voice traffic gets the highest priority, followed by video, best effort, and background traffic, in this order.
RADIUS	Remote Authentication Dial In User Service This is a networking protocol that provides Authentication, Authorization, and Accounting (AAA) management for remote users. The RADIUS provides centralized management of usernames and passwords.

SNMP Simple Network Management Protocol

This is an Internet-standard protocol for managing devices on IP networks. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

SSID Service Set Identifier

This is also known as the ESSID or the wireless network name.

Station A device that connects wirelessly to an access point.

Subnet A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 192.168.7 belong to the same subnet.

TCP Transmission Control Protocol

This is a protocol for transmitting data over the Internet with guaranteed reliability and in-order delivery.

UDP User Datagram Protocol

This is a protocol for transmitting data over the Internet quickly but with no guarantee of reliability or in-order delivery.